世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
G06F 17/60, 17/30, 15/00

A1

(11) 国際公開番号 WO99/59092

(43) 国際公開日 1999年11月18日(18.11.99)

(21) 国際出願番号 PCT/JP99/02404

(22) 国際出願日 1999年5月10日(10.05.99)

(30) 優先権データ
特願平10/127227 1998年5月11日(11.05.98) JP

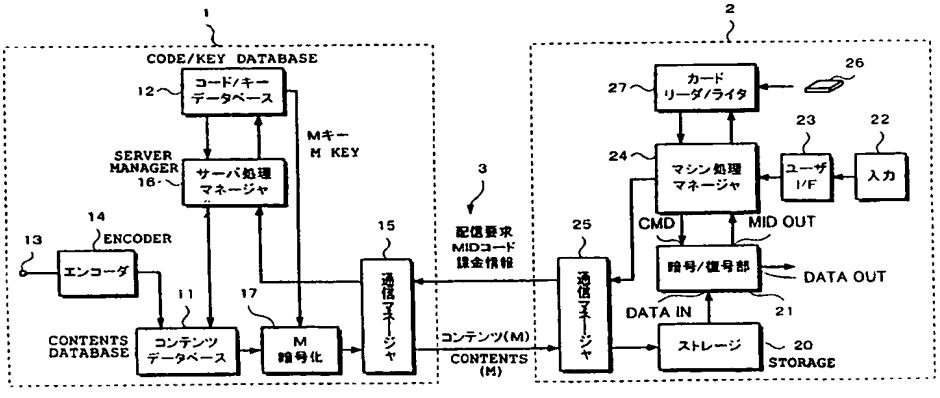
(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
勝又 泰(KATSUMATA, Yasushi)[JP/JP]
大林正之(OHBAYASHI, Masayuki)[JP/JP]
中津山孝(NAKATSUYAMA, Takashi)[JP/JP]
韓 敏哉(KAN, Toshiya)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
弁理士 杉浦正知(SUGIURA, Masatomo)
〒170-0013 東京都豊島区東池袋1丁目48番10号
25山京ビル420号 Tokyo, (JP)

(81) 指定国 CN, IN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

添付公開書類
国際調査報告書

(54)Title: APPARATUS FOR DATA DISTRIBUTION, AND TERMINAL FOR DATA DISTRIBUTION

(54)発明の名称 データ配信装置及びデータ配信用の端末装置



3 ... INFORMATION REQUEST
MID CODE
CHARGE INFORMATION
15 ... COMMUNICATION MANAGER
17 ... M ENCRYPTION
21 ... ENCRYPTION/DECRYPTION SECTION
22 ... INPUT
24 ... MACHINE MANAGER
25 ... COMMUNICATION MANAGER
27 ... CARD READER/WRITER
23...USER I/F

(57) Abstract

A contents server comprises a contents database that stores the data of contents encrypted with a C key and the C key. The data of contents encrypted with the C key, together with the C key, are encrypted with an M key, and sent to a user machine. In the user machine, the data of contents encrypted with the C key and the C key are stored in a storage device. For reproduction, the data of contents encrypted with the C key and the C key are sent from the storage device to an encryption/decryption section and decrypted. The user is charged on the basis of the C key. A DA code, which changes dynamically with time, is appended to the C key.

(57)要約

コンテンツサーバには、Ｃキーにより暗号化されたコンテンツのデータと、Ｃキーとが蓄積されるコンテンツデータベースを設ける。Ｃキーにより暗号化されたコンテンツのデータと、Ｃキーを、Ｍキーで暗号化して、ユーザマシンに送る。ユーザマシンでは、Ｃキーにより暗号化されたコンテンツのデータと、Ｃキーをストレージデバイスに保存する。再生時にストレージデバイスからのＣキーにより暗号化されたコンテンツのデータと、Ｃキーを、暗号化／復号化処理部に送り、復号すると共に、Ｃキーに応じて課金を行なう。また、Ｃキーに、時間と共に動的に変化するＤＡコードを付加する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AL	アルバニア	EE	エストニア	LC	セントルシア	SD	スーダン
AM	アルメニア	ES	スペイン	LI	リヒテンシュタイン	SE	スウェーデン
AT	オーストリア	FI	フィンランド	LK	スリ・ランカ	SG	シンガポール
AU	オーストラリア	FR	フランス	LR	リベリア	SI	スロヴェニア
AZ	アゼルバイジャン	GA	ガボン	LS	レソト	SK	スロヴァキア
BA	ボズニア・ヘルツェゴビナ	GB	英国	LT	リトアニア	SL	シエラ・レオネ
BB	バルバドス	GD	グレナダ	LU	ルクセンブルグ	SN	セネガル
BE	ベルギー	GE	グルジア	LV	ラトヴィア	SZ	スワジランド
BF	ブルギナ・ファソ	GH	ガーナ	MA	モロッコ	TD	チャード
BG	ブルガリア	GM	ガンビア	MC	モナコ	TG	トーゴー
BJ	ベナン	GN	ギニア	MD	モルドヴァ	TJ	タジキスタン
BR	ブラジル	GW	ギニア・ビサオ	MG	マダガスカル	TZ	タンザニア
BY	ベラルーシ	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア共和国	TM	トルクメニスタン
CA	カナダ	HR	クロアチア	ML	マリ	TR	トルコ
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	TT	トリニダッド・トバゴ
CG	コンゴー	ID	インドネシア	MR	モーリタニア	UA	ウクライナ
CH	スイス	IE	アイルランド	MW	マラウイ	UG	ウガンダ
CI	コートジボアール	IL	イスラエル	MX	メキシコ	US	米国
CM	カメルーン	IN	インド	NE	ニジェール	UZ	ウズベキスタン
CN	中国	IS	アイスランド	NL	オランダ	VN	ヴィェトナム
CR	コスタ・リカ	IT	イタリア	NO	ノールウェー	YU	ユーゴースラビア
CU	キューバ	JP	日本	NZ	ニュー・ジーランド	ZA	南アフリカ共和国
CY	キプロス	KE	ケニア	PL	ポーランド	ZW	ジンバブエ
CZ	チェッコ	KG	キルギスタン	PT	ポルトガル		
DE	ドイツ	KP	北朝鮮	RO	ルーマニア		
DK	デンマーク	KR	韓国				

明　細　書

データ配信装置及びデータ配信用の端末装置

技術分野

この発明は、例えば、複数の音楽データが蓄積されるコンテンツサーバと、このコンテンツサーバに蓄積されたコンテンツから所望のコンテンツが配信されるユーザマシンとからなる情報配信システムに関するもので、特に、コンテンツの保護と課金に係わる。

背景技術

近年、インターネットや衛星通信の普及により、コンピュータネットワーク網を利用した種々のサービスが実現されつつある。そのようなコンピュータネットワーク網を使ったサービスのひとつとして、以下のような音楽配信サービスを行なうシステムが提案されている。

第１４図において、５０１はコンテンツサーバ、５０２はユーザマシンである。コンテンツサーバ５０１には、複数の音楽データがコンテンツとして蓄積されている。ユーザマシン５０２には、ハードディスクドライブや光ディスクドライブ等のストレージデバイス５０４が接続されると共に、課金を行なうためのカードリーダ／ライタ５０５が接続される。カードリーダ／ライタ５０５には、カード５０６が装着される。

音楽配信サービスを利用する場合には、ユーザマシン５０２が伝送路５０３を介してコンテンツサーバ５０１に接続される。伝送路５０３は、例えば、インターネットのようなコンピュータネットワーク網である。ユーザマシン５０２がコンテンツサーバ５０１に接続されると、コンテンツサーバ５０１からユーザマシン５０２にコンテンツのリストや検

索画面が送られる。

ユーザは、このコンテンツのリストや検索画面で所望のコンテンツを検索して、ダウンロードしたいコンテンツを選択する。ユーザがコンテンツを選択すると、ユーザマシン５０２からコンテンツサーバ５０１にそのコンテンツの要求命令が送られる。コンテンツサーバ５０１で、要求命令に応じてコンテンツが取り出され、このコンテンツがコンテンツサーバ５０１からユーザマシン５０２に送られる。そして、このコンテンツがユーザマシン５０２のストレージデバイス５０４に保存される。このとき、カードリーダ／ライタ５０５により、適切な課金が行なわれる。

このような音楽配信システムが普及すると、ユーザは、所望の楽曲の音楽データを通信で簡単に入手することができる。また、このようなシステムにおけるサーバには、検索機能が備えられており、このような検索機能を使うと、所望の楽曲を検索して、入手することが簡単にできる。更に、このようなシステムにおけるサーバでは、常に音楽データの更新が行われるため、最新の楽曲をいち早く入手することができる。

ところが、このようにサーバからの音楽データをユーザマシンに配信するようなシステムでは、コンテンツのデータが無断で複製され、著作者の権利が守られなくなる危険性がある。このため、コンテンツのデータが無断で複製されることがないように、複製防止のための機能を付加する必要があると共に、コンテンツに対して適切な課金が行なわれる必要がある。

また、このようなシステムでは、ダウンロードした音楽データを他の機器で再生させたり、他人譲渡したりするようなことが考えられる。常に、１台の機器にのみコンテンツのデータが移動されるようにすれば、不正コピーが出回る可能性はない。ところが、他の機器への複製を一切

禁止してしまうと、このようなコンテンツのデータの移動も行なえなくなってしまう。

したがって、この発明の目的は、コンテンツの配信を行なうようなシステムで、コンテンツの保護が十分図れ、正当な課金が行なえるようにした情報配信システムを提供することにある。

発明の開示

この発明は、機器固有の第１の識別データと第１の識別データと対応する第２の識別データとが記憶されている第１の記憶部と、

第１の記憶部から読み出された第１の識別データとともにデータの配信要求データを送信するとともに送信されてきたデータを受信する第１の送受信部と、

データ送受信部によって受信されたデータを蓄える第１のデータ記憶部と、

第１のデータ記憶部から読み出されたデータを第１の記憶部に記憶されている第２の識別データに基づいて復号化処理を施す第１の信号処理部と、

第１の送受信部によって受信されたデータを第１のデータ記憶部に記憶させる動作を行うとともに第１のデータ記憶部から読み出されたデータの第１の信号処理部による復号化処理動作を制御する第１の制御部と、

第１の送受信部から送信されてきた第１の識別データと配信要求データを受信するとともにデータの送信を行う第２の送受信部と、

複数のデータが記憶され、配信要求データに対応するデータを出力する第２のデータ記憶部と、

送信されてきた第１の識別データに対応する第２の識別データが記憶さ

れている第２の記憶部と、

第２のデータ記憶部から出力されたデータに第２の記憶部から読み出された第２の識別データに基づいて暗号化処理を施す第２の信号処理部と、

送信されてきた配信要求データと第１の識別データに基づいて第２の記憶部から第２の識別データの読み出し制御を行うとともに配信要求データに基づいて第２のデータ記憶部からデータの読み出し制御を行う第２の制御部とを備え、

第２の送受信部を介して送信されてきた第２の識別データに基づいて暗号化されたデータを第１の信号処理部によって復号するデータ配信装置である。

この発明は、機器固有の第１の識別データと第１の識別データと対応する第２の識別データとが記憶されている第１の記憶部と、第１の記憶部から読み出された第１の識別データとともにデータの配信要求データを送信するとともに送信されてきたデータを受信する第１のデータ送受信部と、データ送受信部によって受信されたデータを蓄える第１のデータ記憶部と、第１のデータ記憶部から読み出されたデータを第１の記憶部に記憶されている第２の識別データに基づいて復号化処理を施す第１の信号処理部と、第１の送受信部によって受信されたデータを第１のデータ記憶部に記憶させる動作を行うとともに第１のデータ記憶部から読み出されたデータの第１の信号処理部による復号化処理動作を制御する第１の制御部とを有する少なくともひとつの端末機器部と、

端末機器部と伝送路を介して接続され、第１の送受信部から送信されてきた第１の識別データと配信要求データを受信するとともにデータの送信を行う第２の送受信部と、複数のデータが記憶され、配信要求データに対応するデータを出力する第２のデータ記憶部と、送信されてきた

第1の識別データに対応する第2の識別データが記憶されている第2の記憶部と、第2のデータ記憶部から出力されたデータに第2の記憶部から読み出された第2の識別データに基づいて暗号化処理を施す第2の信号処理部と、送信されてきた配信要求データと第1の識別データに基づいて第2の記憶部から第2の識別データの読み出し制御を行うとともに配信要求データに基づいて第2のデータ記憶部からデータの読み出し制御を行う第2の制御部とを有するサーバ装置部とを備え、

第2の送受信部を介して送信されてきた第2の識別データに基づいて暗号化されたデータを第1の信号処理部によって復号するデータ配信装置である。

この発明は、装置固有の第1の識別データと第1の識別データと対応する第2の識別データとが記憶されている記憶部と、

記憶部から読み出された第1の識別データとともにデータの配信要求データを送信するとともに第2の識別データによって暗号化されて送信されてきたデータを受信するデータ送受信部と、

データ送受信部によって受信された第2の識別データに基づいて暗号化されたデータを蓄えるデータ記憶部と、

データ記憶部から読み出されたデータを記憶部に記憶されている第2の識別データに基づいて復号処理を施す信号処理部と、

送受信部によって受信されたデータをデータ記憶部に記憶させる動作を行うとともにデータ記憶部から読み出されたデータの信号処理部による復号化処理動作を制御する制御部とを備えているデータ配信用の端末装置である。

図面の簡単な説明

第1図はこの発明が適用できるデータ配信システムにおけるMキーを

用いたシステムの説明に用いるブロック図である。第２図はこの発明が適用できるデータ配信システムにおけるＭキーを用いたシステムの暗号化／復号化処理部の説明に用いるブロック図である。第３図はこの発明が適用できるデータ配信システムにおけるＣキーを用いたシステムの説明に用いるブロック図である。第４図はこの発明が適用できるデータ配信システムにおけるＣキーを用いたシステムの暗号化／復号化処理部の説明に用いるブロック図である。第５図はこの発明が適用できるデータ配信システムにおけるＣキーを用いたシステムの説明に用いるフローチャートである。第６図はこの発明が適用できるデータ配信システムにおけるＴキーを用いたシステムの説明に用いるブロック図である。第７図はこの発明が適用できるデータ配信システムにおけるＴキーを用いたシステムの暗号化／復号化処理部の説明に用いるブロック図である。第８図Ａ及び第８図Ｂはこの発明が適用できるデータ配信システムにおけるＴキーを用いたシステムにおける暗号化／復号化処理部の説明に用いるブロック図である。第９図はこの発明が適用できるデータ配信システムにおけるＤＡコードを用いたシステムの説明に用いるブロック図である。第１０図はＤＡコードの説明に用いる略線図である。第１１図はこの発明が適用できるデータ配信システムにおけるＤＡコードを用いてシステムの暗号化／復号化処理部の説明に用いるブロック図ある。第１２図はこの発明が適用できるデータ配信システムにおけるＤＡコードを用いたシステムの説明に用いるフローチャートである。第１３図はこの発明が適用できるデータ配信システムにおけるＤＡコードを用いたシステムの説明に用いるフローチャートである。第１４図は従来のデータ配信システムの一例のブロック図である。

発明を実施するための最良の形態

以下、この発明の実施の形態について図面を参照して説明する。この発明は、コンテンツのデータを転送するようなシステムにおいて、コンテンツのデータの保護が図れると共に、適切な課金が行なえるようにしたものである。このようなシステムにで用いられる暗号化キーやコードについて先ず簡単に説明しておく。

1．キー及びコードの説明

この発明が適用されたシステムでは、以下のような暗号化キーやコードが用いられる。

（1）Mキー

M（Machine）キーの役割は、特定の機器、後述するユーザーマシンでのみデータを利用可能とすることである。Mキーは例えば機器の工場出荷時に各機器毎に与えられるもので、各機器固有の暗号化情報である。Mキーは、保護を図るために、例えば機器の暗号化／復号化処理部内に埋め込まれ、機器内から外へは取り出せないようになっている。

（2）ＭＩＤコード

各機器には、固有のＭＩＤ（Machine Idnetification）コードが付与される。このＭＩＤコードも、工場出荷時に各機器に付与される。ＭＩＤコードは、各機器を特定するためにのみ使用されるものであり、直接的に暗号化キーとして用いられるものではない。したがって、外部に漏れても、データの保護が守られなくなる危険性は少ない。ＭＩＤコードは、Mキーと同様に、例えば機器の暗号化／復号化処理部内に埋め込んでおいても良いし、別のＲＯＭやＥＥＰＲＯＭに蓄えておいても良い。

（3）Ｃキー

C（Contents）キーの役割は、各コンテンツ毎にデータの保護を図ることである。ここで、コンテンツとは、移動できる１かたまりの情報の

単位とする。すなわち、データを課金するようなシステムでは、１つの課金の対象となる情報の単位である。音楽サーバのような場合には、１曲毎に課金をするとすると、各曲の音楽データという単位が１つのコンテンツのデータとなる。

各コンテンツは、各コンテンツに固有のＣキーを用いて暗号化される。したがって、そのコンテンツに対応するＣキーを有しているユーザ側の機器でのみ、そのＣキーを使ってコンテンツの暗号を解読して、再生することが可能である。このように、Ｃキーを有しているユーザ側の機器でのみ、そのコンテンツを利用可能なことから、Ｃキーは、そのコンテンツを利用できる権利を表すキーという見方もできる。

（４）Ｔキー

Ｔ（Transfer）キーの役割は、各ユーザ機器間でデータの移動を行う際に、データの保護を図るためのものである。各機器間でコンテンツの移動を行うような場合に、Ｃキーが外部に漏れる可能性がある。このため、各機器間でデータの移動を行う場合には、Ｃキーと、Ｃキーで暗号化されたコンテンツは、更に、Ｔキーで暗号化される。

Ｔキーは、データの受け取り側の機器と、データの送り側の機器との間で予め決められたアルゴリズムで、ＭＩＤコードに基づいて生成される。すなわち、機器間でコンテンツのデータの移動を行う場合には、受け取り側の機器から送り側の機器に対して、受け取り側のＭＩＤコードが送られる。送り側の機器では、送られてきたＭＩＤコードに基づいて、Ｔキーが生成される。また、受け取り側の機器では、自分のＭＩＤコードに基づいて、同様のアルゴリズムによりＴキーが生成される。

（５）ＤＡコード

暗号／復号化チップ内で生成される動的認証コードであり、Ｃキーに付加される。ＤＡコードは、例えば、乱数、タイムコード等を利用して

生成される。このようなDAコードを付加しておくと、Cキーを一時的に退避させてコンテンツを不正使用することができなくなる。また、DAコードを利用して、所定の期間使用を許可／禁止したり、コンテンツを貸し借りしたりすることができるようになる。

2．Mキーを使ったシステムについて

第1図は、この発明が適用されたデータ配信システムの一例を示すものである。この例は、Mキーと呼ばれる暗号化キーを導入して、特定の端末機器でのみデータを利用可能にするようにしたものである。

第1図において、コンテンツサーバ1は伝送路3によってユーザマシン2と結ばれている。尚、第1図ではコンデンツサーバ1に伝送路3を介して接続される端末機器としてのユーザマシン2は説明を簡単にするために1個しか描かれていないが、実際にはサーバ1に伝送路3を介して複数のユーザマシン2が接続される。コンテンツサーバ1には、コンテンツデータベース11が設けられる。このコンテンツデータベース11には、コンテンツサーバ1で提供するコンテンツのデータが格納されている。

コンテンツデータベータ11に格納されるコンテンツのデータは、コンテンツ入力端子13から入力、供給される。例えば、音楽配信サービスを行なうサーバの場合には、コンテンツ入力端子13から音楽データが供給される。この音楽データは、エンコーダ14に供給される。エンコーダ14で、この音楽データが例えば、特開平3－139923号や特開平3－139922号等に開示されている変形DCT（Modified Discreat Transform）：所謂ATRAC（Adaptive Transform Acoustic Coding）で圧縮符号化される。この圧縮された音楽データがコンテンツデータベース11に蓄えられる。

コンテンツサーバ1には、RAMやハードディスクドライブから構成

されるコード及びキーデータベース１２が設けられる。このコード及びキーデータベース１２には、コンテンツサーバ１に繋がれる全ての機器としてのユーザマシン２のＭＩＤコードとＭキーとが蓄えられる。ＭＩＤコードは、各ユーザマシン２を識別するためのユーザマシン毎の固有の情報である。Ｍキーは、各ユーザマシン毎に固有の暗号化キーである。ＭＩＤコード及びＭキーは例えば機器の工場出荷時に各ユーザマシン２に与えられる。ＭＩＤコード及びＭキーを工場出荷時に各ユーザマシン２に付与する際に、各機器毎に付与したＭＩＤコード及びＭキーのリストに基づいてコード及びキーデータベータ１２に記憶されるデータが生成される。

コンテンツサーバ１の全体動作は、サーバ処理マネージャ１６により管理されている。コンテンツサーバ１の通信制御は、通信マネージャ１５により管理されている。コンテンツサーバ１からのデータは、暗号化回路１７により暗号化される。このときの暗号化は、ユーザマシン２から送られてきたＭＩＤコードに基づいてコード及びキーデータベース１２で検索されたＭキーに基づいて行なわれる。

一方、端末機器としてのユーザマシン２には、暗号化／復号化処理部２１が設けられる。この暗号化／復号化処理部２１は、データの暗号化処理及び暗号の復号化処理を行う専用のＩＣより構成されている。この暗号化／復号化処理部２１には、工場出荷時に、機器固有のＭＩＤコードと、Ｍキーが格納されている。

第２図は、暗号化／復号化処理部２１の構成を示すものである。暗号化／復号化処理部２１には、Ｍキーホルダ５１と、ＭＩＤコードホルダ５２と、Ｍキー復号化回路５３と、コントローラ５４が設けられる。Ｍキーホルダ５１には、各機器固有の暗号化情報であるＭキーが工場出荷時に記憶される。ＭＩＤコードホルダ５２には、各機器固有の識別情報

である M I D コードが工場出荷時に記憶される。コントローラ５４は、暗号化／復号化処理部２１の動作を制御している。

コントローラ５４には、後述するマシンマネジャから送信されてくるコマンドがコマンド端子ＣＭＤに供給される。このコマンドに基づいて、暗号化／復号化処理部２１の動作が設定される。Ｍキー復号化回路５３には、入力端子ＤＡＴＡ＿ＩＮからＭキーで暗号化されたコンテンツのデータが供給される。Ｍキー復号化回路５３には、Ｍキーホルダ５１からＭキーが供給される。Ｍキー復号化回路５３で、入力端子ＤＡＴＡ＿ＩＮから入力コンテンツのデータの暗号解読を行なわれる。Ｍキー復号回路５３の出力データは、データ出力端子ＤＡＴＡ＿ＯＵＴから出力される。ＭＩＤコードホルダ５２からは、コード出力端子ＭＩＤ＿ＯＵＴが導出される。このコード出力端子ＭＩＤ＿ＯＵＴからは、ＭＩＤコードが出力される。

第２図に示すように、暗号化／復号化の処理は、１チップのＩＣから構成される暗号化／復号化処理部２１で行われ、この暗号化／復号化処理部２１内に、Ｍキーと、ＭＩＤコードが格納されている。このため、外部からは、暗号化／復号化処理部２１での暗号処理がどのようにして行われ、暗号化キーが何であるのかは解明できない。

第１図において、ユーザマシン２には、入力部２２からユーザによって操作された結果としての入力が供給される。入力部２２からの入力は、ユーザインターフェース２３を介して、マシン処理マネージャ２４に与えられる。

マシン処理マネージャ２４は、マイクロコンピュータ等から構成され、ユーザマシン２の全体処理を行っている。マシン処理マネージャ２４は、入力部２２からコンテンツサーバ１のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理部２１にコマンドを与え、ＭＩＤ

コードを問い合わせる動作を行なう。暗号化／復号化処理部２１は、ＭＩＤコードの問い合わせコマンドが供給されると、供給されたＭＩＤの問い合わせコマンドに対応して、ＭＩＤコードホルダ５２（第２図）に記憶されているＭＩＤコードをマネージャ２４に出力する。

マシン処理マネージャ２４は、暗号化／復号化処理部２１からＭＩＤコードを受け取ったら、通信マネージャ２５に、配信要求と、ＭＩＤコードと、課金情報を送る。これら配信要求、ＭＩＤコード、課金情報は、通信処理マネージャ２５から、伝送路３を介して、ユーザマシン２からコンテンツサーバ１の通信マネージャ１５に送られる。

コンテンツサーバ１からのコンテンツのデータの配信サービスを受ける場合には、カード２６が装着される。このカード２６の残高情報がカードリーダ／ライタ２７を介してマシン処理マネージャ２４に送られる。コンテンツの配信が実行されると、マシン処理マネージャ２４は、カードリーダ／ライタ２７を介して、カード２６に、引き出し指示、もしくは減額指示を与え、カード２６から、コンテンツの配信に応じた代金が差し引かれる。このようにして、コンテンツにの配信に対する代金の支払いがコンテンツ配信を行っている会社に対して行なわれる。このとき、正規のユーザか否か、ユーザが確かに課金を行っているか否かをチェックしてから、ユーザマシン２２から送信されてきたＭＩＤコードに対応するＭキーを出力させるようにしても良い。

コンテンツサーバ１側では、マイクロコンピュータなどから構成されるサーバ処理マネージャ１６がサーバ１の全体処理の制御を行なっている。通信マネージャ１５がユーザマシン２から送信されてくる配信要求、ＭＩＤコード、課金情報を受信すると、受信した配信要求、ＭＩＤコード、課金情報は、サーバ処理マネージャ１６に送られる。

サーバ処理マネージャ１６は、ユーザマシン２送信されてきたＭＩＤ

コードを受信したら、このＭＩＤコードをコード及びキーデータベース１２に送り、ユーザマシン２から送信されてきたＭＩＤコードに対応するユーザマシンのＭキーを問い合わせるコマンドをベース１２に供給する。コード及びキーデータベース１２は、前述したようにサーバ１に接続される各機器毎のＭＩＤコードと、ＭＩＤコードに対応するＭキーの情報が予め格納されており、コード及びキーデータベース１２は、マネージャ１６から送信されてきたＭＩＤコードを受け付けると、送信されてきたＭＩＤコードからユーザマシン２を識別し、ＭＩＤコードを送信してきたユーザマシン２に対応するＭキーを出力する。送信されてきたＭＩＤコードに対応するＭキーは、Ｍキー暗号化回路１７に送られる。ベース１２から送信されてきたＭキーに基づいてＭキー暗号化回路１７に、暗号化キーがセットされる。

サーバ処理マネージャ１６は、ユーザマシン２からの配信要求を受け付けると、要求されたコンテンツの配信指示を示すコマンドをコンテンツデータベース１１に送る。コンテンツデータベース１１は、ユーザマシン２の配信指示を受け取ると、送信されてきた配信指示に対応するコンテンツのデータの読み出しを行なう。データベース１１から読み出されたコンテンツのデータは、Ｍキー暗号化回路１７に送られる。

Ｍキー暗号化回路１７には、コード及びキーデータベース１２から、データを要求したユーザマシン２の機器のＭＩＤコードに対応したＭキーがセットされている。コンテンツデータベース１１から送られるコンテンツのデータは、Ｍキー暗号化回路１７で、上述したユーザマシン２のＭＩＤコードに対応するＭキーにより暗号化される。Ｍキーで暗号化されたコンテンツのデータは、コンテンツサーバ１の通信マネージャ１５から、伝送路３を介して、ユーザマシン２の通信路マネージャ２５に送られる。このコンテンツのデータは、ユーザマシン２にあるストレー

ジデバイス２０に蓄積される。ここで、伝送路３としては、ＩＳＤＮ（Integrated Servises Digital Network）等の有線又は無線の通信網を伝送路として用いることができる。

このように、ユーザマシン２からコンテンツサーバ１にコンテンツの配信を要求する際に、ユーザマシン２からコンテンツサーバ１に、ユーザマシン２の機器固有のＭＩＤコードが送られる。コンテンツサーバ１には、コード及びキーデータベース１２が設けられており、このコード及びキーデータベース１２から、ユーザマシン２から送られてきたユーザマシン２のＭＩＤコードに対応するＭキーが呼び出され、データベース１１から読み出されたコンテンツのデータがこのＭキーで暗号化される。ユーザマシン２の機器固有のＭキーで暗号化されたコンテンツのデータがユーザマシン２に送られ、暗号化されたコンテンツのデータがユーザマシン２のストレージデバイス２０に蓄えられる。ストレージデバイス２０に蓄えられたコンテンツのデータは、ユーザマシン２の機器固有のＭキーで暗号化されているので、コンテンツの配信を要求したユーザマシン２以外では配信されてきたコンテンツのデータの復号が行なえない。これにより、サーバ１からユーザマシン２に配信されるコンテンツの著作権を守ることができる。

すなわち、ストレージデバイス２０に蓄えられたコンテンツのデータを復号する場合には、ストレージデバイス２０から、読み出されたコンテンツのデータは第２図における暗号化／復号化処理部２１のデータ入力端子ＤＡＴＡ＿ＩＮに供給される。第２図に示したように、暗号化／復号化処理部２１のＭキーホルダ５１には、ユーザマシン２の機器固有のＭキーが蓄えられている。コンテンツサーバ１から送られてきたコンテンツのデータは、ＭＩＤコードホルダ５２のＭＩＤコードに対応するＭキーで暗号化されているため、コンテンツサーバ１側のＭキー暗号化

回路17に設定されたMキーは、ユーザマシン2のMキーホルダ51に格納されているMキーと同様である。したがって、ストレージ20から読み出されたMキーで暗号化されたコンテンツのデータは、暗号化／復号化処理部21で、復号することができる。

これに対して、ストレージデバイス20に蓄えられていたコンテンツのデータを、ユーザマシン2以外のユーザマシン又は機器に複製したとする。ストレージデバイス20に蓄えられていたコンテンツのデータは、ユーザマシン2の機器固有のMキーで暗号化されている。他の機器の暗号化／復号化処理部21は、複製元となるユーザマシン2の機器と同じのMキーを有していない。このため、ストレージデバイス20に蓄えられていたコンテンツのデータを本来のユーザマシン2、即ちサーバ1に配信要求を送ってサーバ1から送信されてきたコンテンツのデータを蓄えていたユーザマシン2以外の機器に複製したとしても、複製元となる機器では、コンテンツのデータの暗号を解読できない。

3．Cキーを使ったシステムについて

第1図及び第2図に示すMキーを導入することで、特定の機器でのみコンテンツのデータが利用可能となる。ところが、Mキーだけでは、サーバ1から配信されてきたコンテンツのデータを記憶したユーザマシンからコンテンツのデータを他のユーザマシンや機器に移動させることが一切できなくなってしまう。コンテンツのデータが限りなく複製されてしまうと著作者の権利が守られなくなることが考えられるが、コンテンツのデータが移動されただけなら、コンテンツのデータを利用する機器が移っただけなので、問題は生じない。上述した第1図、第2図に示すように、Mキーだけを用いる装置、方法では、上述したようなコンテンツのデータの或る機器から他の機器、すなわち、或るユーザマシンから他のユーザマシンへの移動に対応できない。ユーザマシンに一度蓄積し

ておいたコンテンツのデータがエラーになってしまったり、ダウンロードに失敗したりするようなことが考えられる。このような場合、正規のユーザが正当な課金をしてそのコンテンツのデータの配信を受けているなら、再度、そのコンテンツのデータを配信し直すことが望まれる。コンテンツには有料のコンテンツと無料のコンテンツがあり、Mキーのみでは、コンテンツの種類に応じて適切な課金が行なえない。

上述したように、Mキーを導入することで、各機器としての各ユーザマシンを単位とするコンテンツのデータの保護、不正なコンテンツデータの複製に対する保護は図れるが、Mキーだけでは、各コンテンツ毎のデータの保護を図り、適切な課金を行なうには不十分である。そこで、コンテンツ毎の暗号化を行うCキーを導入した例を第3図以下を用いて説明する。

第3図には、Cキーを導入したデータ配信システムの一例が示されている。Cキーの役割は、各コンテンツ毎にデータの保護を図ることである。

Cキーを導入したデータ配信システムにおいては、ユーザマシン102側の暗号化／復号化処理部121として、第2図に示した暗号化／復号化処理部21と同様に、第4図に示すように、Mキーホルダ151と、MIDコードホルダ152と、Mキー復号化回路153と、コントローラ154とが設けられると共に、更に、処理部121には、Cキー取り込み回路155と、Cキー復号化回路156とが設けられる。Mキーホルダ151、MIDコードホルダ152、Mキー復号化回路153、コントローラ154の動作は、前述のMキーのみのデータ配信システムにおける暗号化／復号化処理部21と同様であり、Mキーホルダ151には、各ユーザマシン102の機器固有の暗号化情報であるMキーが工場出荷時に記憶され、MIDコードホルダ152には、各ユーザマシン

1-0-2の機器固有の識別情報であるM-I-Dコードが工場出荷時に記憶され、コントローラ１５４は、暗号化／復号化処理部１２１の動作を制御している。Ｃキー取り込み回路１５５は、Ｍキーの解読により復号されたＣキーを保持するものである。Ｃキー復号回路１５６は、Ｃキーによる復号化処理を行なうものである。

コントローラ１５４には、後述するマシン処理マネージャからコマンド端子ＣＭＤからコマンドが供給され、このコマンド端子ＣＭＤから供給されてくるコマンドに基づいて、暗号化／復号化処理部１２１の動作が設定される。Ｍキー復号化回路１５３には、入力端子ＤＡＴＡ＿ＩＮから、Ｃキーで暗号化され更にＭキーで暗号化されたデータと、入力端子ＫＥＹ＿ＩＮからのＭキーで暗号化されたＣキーが供給される。Ｍキー復号化回路１５３には、Ｍキーホルダ５１から、Ｍキーが供給される。

入力データの暗号化キー、すなわち、ＤＡＴＡ＿ＩＮから供給されるデータを暗号化しているＭキーがＭキーホルダ１５１からのＭキーと一致していれば、Ｍキー復号化回路１５３で、暗号解読を行なえる。Ｍキー復号化回路１５３からは、Ｍキーによる暗号化の解かれたＣキーと、Ｃキーで暗号化されたデータが出力される。このＣキーがＣキー取り込み回路１５５に保持され、Ｃキーで暗号化されたデータがＣキー復号化回路１５６に供給される。

Ｃキー復号化回路１５６で、Ｃキーに基づく復号化処理が行なわれ、Ｃキーで暗号化されているデータが解読される。このＣキー復号回路１５６の出力データは、データ出力端子ＤＡＴＡ＿ＯＵＴから出力される。ＭＩＤコードホルダ１５２からは、コード出力端子ＭＩＤ＿ＯＵＴが導出される。このコード出力端子ＭＩＤ＿ＯＵＴからは、ＭＩＤコードが出力される。暗号化／復号化処理部１２１には、Ｃキーで暗号化され

てデータを転送するために、Ｃキーの出力端子ＫＥＹ＿ＯＵＴと、Ｃキーで暗号化されたコンテンツのデータの出力端子ＤＡＴＡ＿Ｔが設けられる。

このように、Ｃキーを導入したデータ配信システムにおいては、第３図におけるユーザマシン１０２側の暗号化／復号化処理部１２１として、第４図に示すような構成のものが用いられる。第３図に示すように、コンテンツサーバ１０１側には、Ｃキーを発生するＣキー生成部１１８と、Ｃキー生成部１１８によって生成されたＣキーを使って、コンテンツのデータを暗号化するＣキー暗号化回路１１９が設けられる。それ以外の構成については、前述の第１図に示したコンテンツサーバ１と同様に構成されている。

前述のＭキーだけのデータ配信システムでは、コンテンツ入力端子１３からのデータは、エンコーダ１４で圧縮符号化されて、そのままコンテンツデータベース１１に蓄積されたが、第３図に示す例では、コンテンツ入力端子１１３からのデータは、エンコーダ１１４で圧縮符号化された後、Ｃキー暗号化回路１１９に送られ、Ｃキー生成部１１８からのＣキーによりＣキー暗号化回路１１８で暗号化されて、コンテンツデータベース１１１に蓄積される。このときの暗号化回路１１９で用いられたＣキーがコンテンツデータベース１１１に蓄積される。

ユーザがコンテンツサーバ１０１のコンテンツの配信を受けたい場合には、ユーザがユーザマシン１０２の入力部１２２を操作してユーザインターフェース１２３を介して、マシン処理マネージャ１２４にコンテンツ配信を指示する入力が与えられる。

マシン処理マネージャ１２４は、入力部１２２からコンテンツサーバ１０１のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理部１２１にコマンドを与え、ＭＩＤコードを問い合わせる。暗号化

／復号化処理部１２１は、マシン処理マネージャ１２４から送信されてきたコマンドが与えられると、このコマンドに対応して、ＭＩＤコードを出力する。

マシン処理マネージャ１２４は、暗号化／復号化処理部１２１からＭＩＤコードを受け取ったら、通信マネージャ１２５に、配信要求と、ＭＩＤコードと、課金情報を送る。配信要求、ＭＩＤコード及び課金情報の各情報は、通信処理マネージャ１２５から、伝送路１０３を介して、コンテンツサーバ１０１の通信マネージャ１１５に送られる。

通信マネージャ１１５は、ユーザマシン１０２からのＭＩＤコードが供給されると、供給されたＭＩＤコードをサーバマネージャ１１６に送る。サーバマネージャ１１６は、コード及びキーデータベース１１２にユーザマシン１０２から送信されてきたＭＩＤコードを送り、送信されてきたＭＩＤコードに対応するＭキーを問い合わせるコマンドを送信する。コード及びキーデータベース１１２は、ユーザマシン１０２から送信されてきたＭＩＤコードに対応する機器のＭキーを出力する。コード及びキーデータベース１１２から出力されるＭキーは、Ｍキー暗号化回路１１７に供給され、Ｍキー暗号化回路１１７にユーザマシン１０２から送信されてきたＭＩＤコードに対応するＭキーがセットされる。

サーバ処理マネージャ１１６は、ユーザマシン１０２からの配信要求を受け付けると、要求されたコンテンツの配信指示のコマンドをコンテンツデータベース１１１に送る。コンテンツデータベース１１１は、サーバ処理マネージャ１１６からの情報に基づいて、ユーザマシン１０２の配信要求と対応するコンテンツのデータを読み出す。

前述したように、コンテンツデータベース１１１のデータは、Ｃキーにより暗号化されている。したがって、Ｃキーにより暗号化されたコンテンツデータが、更に、Ｍキー暗号化回路１１７により、Ｍキーで暗号

化される。また、このときのＣキーがコンテンツデータベース１１１から読み出され、Ｍキー暗号化回路１１７により、Ｍキーにより暗号化される。

このように、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータと、Ｍキーで暗号化されたＣキーは、コンテンツサーバ１０１の通信マネージャ１１５から、伝送路１０３を介して、ユーザマシン１０２の通信路マネージャ１２５に送られる。伝送路１０３を介してサーバ１０１より送信されてきたＣキーで暗号化され更にＭキーで暗号化されたコンテンツのデータと、Ｍキーで暗号化されたＣキーは、ユーザマシン１０２のストレージデバイス１２０に蓄積される。

このように、コンテンツデータベース１１１に蓄えられているコンテンツのデータはＣキーで暗号化されており、コンテンツサーバ１０１からユーザマシン１０２にデータが送られる際に、更に、Ｃキーで暗号化されたデータは、Ｍキーで暗号化されている。Ｃキーで暗号化されたコンテンツのデータを解読するためには、Ｃキーが必要であるが、このＣキーは、コンテンツサーバ１から、Ｍキーで暗号化されてユーザマシン１０２に供給されている。

ストレージデバイス１２０に蓄えられたコンテンツのデータを復号する場合には、ストレージデバイス１２０から読み出されたコンテンツのデータは、第４図における暗号化／復号化処理部１２１のデータ入力端子ＤＡＴＡ＿ＩＮに供給される。Ｍキーで暗号化されたＣキーが、ストレージデバイス１２０から読み出されて、暗号化／復号化処理部１２１のキー入力端子ＫＥＹ＿ＩＮに供給される。

第４図に示すように、暗号化／復号化処理部１２１のＭキーホルダ１５１には、ユーザマシン１０２の機器固有のＭキーが蓄えられている。コンテンツサーバ１０１から送られてきたコンテンツのデータは、ＭＩ

Dコードホルダ１５２のＭＩＤコードに対応するＭキーで暗号化されている。コンテンツサーバ１０１側のＭキー暗号化回路１１７に設定されたＭキーは、Ｍキーホルダ１５１に格納されているＭキーと同じである。したがって、ストレージデバイス１２０からの、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータは、Ｍキーに基づく暗号化部分は、Ｍキー復号化回路１５３で、復号することができる。

同様に、ストレージデバイス１２０からのＭキーで暗号化されたＣキーは、Ｍキー復号化回路１５３で復号される。

したがって、Ｍキー復号化回路１５３からは、Ｃキーで暗号化されたデータと、Ｃキーが出力される。このＣキーは、Ｃキー取り込み回路１５５に供給され、Ｃキーで暗号化されたデータは、Ｃキー復号回路１５６に供給される。Ｃキー復号回路１５６で、Ｃキーによる暗号の解読が行なわれ、コンテンツのデータが復号される。この復号されたデータがデータ出力端子ＤＡＴＡ＿ＯＵＴから出力される。Ｃキー取り込み回路１５５から出力されるＣキーがキー出力端子ＫＥＹ＿ＯＵＴから出力される。

このようにコンテンツのデータをＣキーで暗号化しておくと、コンテンツのデータを利用するときには、必ず、これを解読するためのＣキーが必要になる。Ｃキーを有しているユーザ側のユーザマシン又は機器でのみ、コンテンツのデータを利用することができるので、Ｃキーは、そのコンテンツのデータを利用できる権利を表すキーとして用いることができる。

すなわち、１つの端末機器としての或るユーザマシンから他の端末機器としての他のユーサマシンにＣキーを送れば、コンテンツのデータとそのコンテンツのデータを利用する権利が送られたことになり、他のユーザ側の端末機器で、そのコンテンツのデータを利用することができる

。このように１つの端末機器から他のユーザ側の端末機器にＣキーを送った後にその機器のＣキーを消去してしまうと、たとえ送り側の機器にコンテンツのデータが残っていても、そのコンテンツのデータに付加されているＣキーによる暗号を解くことができないので、コンテンツデータは、最早利用できない。換言すると、そのコンテンツデータを他のユーザ側の機器に若しくは他のユーザに譲渡したという見方ができる。

正規のユーザが誤ってコンテンツのデータを消してしまったり、コンテンツのデータのダウンロードに失敗してしまうような場合がある。この場合でも、ユーザマシン１０２にＣキーが残っていれば、そのコンテンツのデータをサーバ１０１より再送してもらい、残っているＣキーを用いて再送してもらったコンテンツのデータを解読し、コンテンツのデータを利用することができる。このように、Ｃキーを導入することにより、以下のように、コンテンツのデータの移動や再送が行なえるようになる。Ｃキーを利用することにより、課金の設定を行なうことができる。

暗号化／復号化処理部１２１のキー出力端子ＫＥＹ＿ＯＵＴからのＣキーと、データの出力端子ＤＡＴＡ＿Ｔからのデータを移動先となる相手側の機器としてのユーザマシンに転送し、データの転送が終わったら、Ｃキー取り込み回路１５５に保存されているＣキー及びストレージデバイス１２０に保存されているＣキーを消去することで、コンテンツのデータの移動が行なわれる。このようにすると、相手側の機器でのみコンテンツのデータの利用が可能となる。このとき、移動元ともるユーザマシンのストレージデバイス１２０に残っているコンテンツのデータは、消去しなくても良い。なぜなら、移動元となるユーザマシンのストレージデバイス１２０に残っているコンテンツのデータは、Ｃキーで暗号化されており、Ｃキーが消去されてしまえば、そ

のコンテンツのデータは解読することができないので、コンテンツのデータとして利用できないからである。

この場合とは逆に、ストレージデバイス１２０のコンテンツのデータを消去してしまった後でも、Ｃキーが保存されていれば、コンテンツのデータをサーバ１０１より再送してもらえれば再びコンテンツのデータの利用ができる。コンテンツのデータの再送は、前述のコンテンツのデータのダウンロードの場合と同様の処理で行なわれる。このとき、新規のコンテンツのデータの配信、すなわち、ダウンロードであるか否かをＣキーで判断し、新規の場合のみ、課金を行なうようにする。例えば、ユーザマシン１０２が送信されてきたＣキーをコンテンツ／Ｃキーデータベース１１１で照合することによって、いつの時点でＣキー生成部１１８で生成されたＣキーであるかによって新規のコンテンツのデータの配信であるか否かを判別する。

上述したように、Ｃキーを使うと、コンテンツのデータの配信の内容に応じた課金が行なえる。例えば、無料のコンテンツのデータに対してはＣキーを付加せず、有料のコンテンツのデータにのみＣキーを付加するようにしても良い。受信側、すなわちユーザマシン１０２側では、サーバ１０１より送られてきたＣキーが新規のものであるか否かをマシン処理マネージャ１２４が判断し、新規のＣキーの場合のみ、課金を行なうようにする。このようにすると、サーバ１０１から送信されてくるＣキーに基づいてサーバ１０１から引き出そうとしているコンテンツ又はコンテンツのデータが有料のコンテンツ又はコンテンツのデータであるか否かを判断することができ、有料のコンテンツ又はコンテンツのデータの保護が図れる。上述のコンテンツのデータの再送のような場合には、ユーザマシン１０２に保存されているＣキーと、受信されたコンテンツのデータを暗号化しているＣキーとを比較し、この比較結果から、上

述したように、課金を行なうかどうかを判断することができる。更に、課金に関する情報（例えば、コンテンツのランク付け等）をコード化してＣキーに包含させておき、同じコンテンツに対して条件により料金を変更できるようにすることも可能である。

第５図は、Ｃキーを使った課金処理を示すフローチャートである。サーバ１０１から配信されてきたデータをユーサマシン１０２のストレージデバイス１２０に取り込む際に、すなわち、ダウンロードの際に、ユーザマシン１０２の暗号化／復号化部１２１のキー出力端子ＫＥＹ＿ＯＵＴより出力されたか否か、すなわち、Ｃキーが受信されたか否かが判断される（ステップＳ１）。Ｃキーが受信されなければ、サーバ１０１から配信されてきたコンテンツのデータが無料のコンテンツのデータであるとして、課金は行なわれない（ステップＳ２）。Ｃキーが受信されたら、ストレージデバイス１２０にＣキーが保存されているか否かが判断される（ステップＳ３）。コンテンツの再送のような場合には、ストレージデバイス１２０にＣキーが保存されているので、受信されたＣキーと、ストレージデバイス１２０に保存されているＣキーとが一致するか否かを判断する（ステップＳ４）。受信されたＣキーと、ストレージデバイス１２０に保存、記憶されているＣキーとが一致している場合には、コンテンツのデータの再送であるので、課金は行なわれない（ステップＳ２）。

ステップＳ３でサーバ１０１から送信されてきたＣキーがストレージデバイス１２０にＣキーが保存されていないと判断された場合、又はステップＳ４で、受信されたＣキーとストレージデバイス１２０に保存されているＣキーとが一致していないと判断された場合には、Ｃキーの課金ランクの情報が取得される（ステップＳ５）。この課金ランクの情報に応じて、課金処理が行なわれる（ステップＳ６）。Ｃキーの課金ラン

ク情報とは、例えばコンテンツのデータの種類やデータの品質を表す情報等が考えられる。

4．Tキーを使ったシステムについて

上述したように、Cキーをデータ配信システムに導入することで、コンテンツのデータの或る機器としてのユーザマシンと他の機器としてのユーザマシンとの間の移動、コンテンツデータの再送が行なえるようになる。ところが、Cキーのみでは、移動先となる相手側の機器にコンテンツの移動を行なう際に、Cキーが直接送信される。このとき、Cキーが外部に漏れて、コンテンツのデータの保護が図られなくなる可能性がある。データ移動時のコンテンツのデータの保護を図るために、Tキーをデータ配信システムに導入した例を以下に説明する。

第6図は、Tキーを導入したデータ配信システムの一例を示すものである。第6図において、データの送り側のユーザマシン202Aは、上述した第3図に示したデータ配信システムのユーザマシン102と同様に、ストレージデバイス220A、暗号化／復号化処理部221A、入力部222A、ユーザインターフェース223A、マシン処理マネージャ224A、通信マネージャ225A、カードリーダ／ライタ227Aから構成される。カードリーダ／ライタ227Aには、上述した第3図に示したデータ配信システムで用いられるカード126と同様のカード226Aが装着される。

データの受信側のユーザマシン202Bは、上述したユーサマシン202Aと同様に前述した第3図に示したデータ配信システムのユーザマシン102のように、ストレージデバイス220B、暗号化／復号化処理部221B、入力部222B、ユーザインターフェース223B、マシン処理マネージャ224B、通信マネージャ225B、カードリーダ／ライタ227Bから構成される。カードリーダ／ライタ227Bには

、上述したカード２２６Ａと同様のカード２２６Ｂが装着される。

Ｔキーを導入したデータ転送システムでは、暗号化／復号化処理部２２１Ａ及び２２１Ｂとして、第７図に示すようなものが用いられる。第７図に示すように、暗号化／復号化処理部２２１Ａ及び２２１Ｂには、Ｍキーホルダ２５１と、ＭＩＤコードホルダ２５２と、Ｍキー復号化回路２５３と、コントローラ２５４と、Ｃキー取り込み回路２５５と、Ｃキー復号化回路２５６とが設けられると共に、Ｔキー暗号化回路２５７と、Ｔキー生成回路２５８、２５９と、Ｔキー復号化回路２６０と、Ｍキー暗号化回路２６１とが設けられる。

Ｍキーホルダ２５１、ＭＩＤコードホルダ２５２、Ｍキー復号化回路２５３、コントローラ２５４の動作は、前述までのデータ配信システムにおけるユーザマシン２、１０２の暗号化／復号化処理部２１、１２１と同様であり、Ｍキーホルダ２５１には、各ユーザマシンの機器固有の暗号化情報であるＭキーが工場出荷時に記憶され、ＭＩＤコードホルダ２５２には、各機器固有の識別情報であるＭＩＤコードが工場出荷時に記憶されている。コントローラ２５４は、暗号化／復号化処理部２２１Ａ、２２１Ｂの動作を制御する。Ｃキー取り込み回路２５５は、Ｍキーの解読により復号されたＣキーを保持し、Ｃキー復号回路２５６は、Ｃキーの復号化処理を行なう。

Ｔキー暗号化回路２５７は、Ｔキー生成回路２５８からのＴキーにより、他の機器としての他のユーザマシン２０２Ｂに或る機器としての或るユーザマシン２０２Ａから移動するデータをＴキーで暗号化するものである。Ｔキー復号回路２６０は、Ｔキー生成回路２５９からのＴキーにより、移動されてきたデータを復号するものである。Ｔキー生成回路２５８及び２５９は、ＭＩＤコードに基づいてＴキーを生成するものである。

第８図Ａ及び第８図Ｂは、ユーザマシン２０２Ａからユーザマシン２０２Ｂに、コンテンツのデータを移動するときの暗号化／復号化処理部２２１Ａ、２２１Ｂの動作を説明するためのものである。

ユーザマシン２０２Ａからユーザマシン２０２Ｂにコンテンツのデータを移動する際には、データを送出する側のユーザマシン２０２Ａから、相手側のユーザマシン２０２ＢにＭＩＤコードの転送要求が送られる。

相手側のユーザマシン２０２Ｂでは、ＭＩＤコードの送信要求を受け付けると、ユーザマシン２０２Ｂの暗号化／復号化処理部２２１ＢのＭＩＤホルダ２５２ＢからＭＩＤコードを呼び出し、ＭＩＤホルダ２５２Ｂから読み出されたＭＩＤコードがコード出力端子ＭＩＤ＿ＯＵＴから出力され、このＭＩＤコードは、ユーザマシン２０２Ｂから、ユーザマシン２０２Ａに送信される。

データを送出する側のユーザマシン２０２Ａでは、コード入力端子ＭＩＤ＿ＩＮから相手側のユーザマシン２０２Ｂから送信されてきたＭＩＤコードを受信すると、受信したＭＩＤコードをＴキー生成回路２５８Ａに供給する。Ｔキー生成回路２５８Ａは、この相手側のユーザマシン２０２Ｂから送られてきたＭＩＤコードに基づいて、Ｔキーを生成する。Ｔキー生成回路２５８Ａで生成されたＴキーがＴキー暗号化回路２５７Ａに供給される。

ユーザマシン２０１Ａは、ユーザマシン２０２ＢからのＭＩＤコードを受信し、Ｔキー暗号化回路２５７Ａに受信したＭＩＤコードに基づいてＴキーが生成され、Ｔキー暗号化回路２５７Ａに供給されたら、ユーザマシン２０１ＡからユーザマシンＢへのコンテンツのデータ及びＣキーの送信をするための動作が開始される。

ユーザマシン２０２Ａのストレージデバイス２２０Ａには、Ｃキーで

暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーが蓄積されている。したがって、ユーザマシン２０２Aからユーザマシン２０２Bにコンテンツのデータ及びCキーを送信する際に、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーが、ユーザマシン２０２Aのストレージデバイス２２０Aから、暗号化／復号化処理部２２１Aのキー入力端子ＫＥＹ＿ＩＮ及びデータ入力端子ＤＡＴＡ＿ＩＮに供給される。

Mキー復号化回路２５３Aには、Mキーホルダ２５１AからMキーが供給される。Mキー復号化回路２５３Aで、Mキーホルダ２５１AからのMキーによりMキーに基づいて施されている暗号の復号処理が行なわれる。このMキー復号回路２５３Aからは、復号化されたCキーとCキーで暗号化されたコンテンツのデータが出力される。復号回路２５３Aから出力されるCキーは、Cキー取り込み回路２５５Aに供給されると共に、Tキー暗号化回路２５７Aに供給される。復号回路２５３Aから出力されるCキーで暗号化されたコンテンツのデータは、Cキー復号化回路２５６Aに供給されると共に、Tキー暗号化回路２５７Aに供給される。

Cキー復号化回路２５６Aで、復号回路２５３Aから供給されるCキーで暗号化されたコンテンツのデータの復号化処理が行なわれ、コンテンツのデータに施されているCキーに基づく暗号の復号化処理が行なわれる。復号されたコンテンツのデータは、データ出力端子ＤＡＴＡ＿ＯＵＴから出力される。

Tキー暗号化回路２５７Aには、Tキー生成回路２５８Aでユーザマシン２０２BのＭＩＤコードに基づいて生成されたTキーが設定されている。Mキー復号回路２５３Aから出力されるCキー及びCキーで暗号

化されたコンテンツのデータは、Ｔキー暗号化回路２５７Ａで、相手側のユーザマシン２０２ＢのＭＩＤコードに基づいて生成されたＴキーで暗号化される。したがって、Ｔキー暗号化回路２５７Ａからは、Ｔキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＴキーで暗号化されたコンテンツのデータが出力される。

このＴキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＴキーで暗号化されたコンテンツのデータは、キー出力端子ＴＫＥＹ＿ＯＵＴ及びデータ出力端子ＴＤＡＴＡ＿ＯＵＴから出力され、相手側のユーザマシン２０２Ｂに送られ、相手側のユーザマシン２０２Ｂの暗号化／復号化処理部２２１Ｂのキー入力端子ＲＣＫＥＹ＿ＩＮ及びデータ入力端子ＲＤＡＴＡ＿ＩＮに入力され、Ｔキー復号化回路２６０Ｂに供給される。ユーザマシン２０２ＢにＴキーで暗号化されたＣキーとＣキー及びＴキーで暗号化されたコンテンツのデータの送信が完了した時点で、ユーザマシン２０２Ａのストレージデバイス２２０Ａに記憶されているＣキーは削除され、ストレージデバイスからのコンテンツのデータの読み出しが禁止される。

Ｔキー復号化回路２６０Ｂには、Ｔキー生成回路２５９Ｂから、Ｔキーが与えられる。このＴキーは、Ｔキー生成回路２５９ＢでＭＩＤホルダ２５２ＢからのＭＩＤコードに基づいて生成されている。

送り側のユーザマシン２０２Ａでは、ユーザマシン２０２Ｂから送信されてくるＭＩＤコードを受信し、Ｔキー生成回路２５８Ａで、受信したＭＩＤコードに基づいて、Ｔキーを生成している。受信側のユーザマシン２０２ＢのＴキー復号化回路２６０Ｂでは、ＭＩＤコードホルダ２５２ＢからのＭＩＤコードに基づいてＴキーを生成している。Ｔキー生成回路２５８ＡとＴキー生成回路２５９Ｂには、同一のＭＩＤコードが送られている。したがって、ユーザマシン２０２Ａから送られてきたＴ

キーによって各々暗号化されているコンテンツのデータ及びＣキーは、ユーザマシン２０２ＢのＴキー復号回路２６０Ｂで復号化することができる。

Ｔキー復号化回路２６０Ｂからは、Ｃキーと、Ｃキーで暗号化されたコンテンツのデータが出力される。このＣキーと、Ｃキーで暗号化されたコンテンツのデータは、Ｍキー暗号化回路２６１Ｂに供給される。

Ｍキー暗号化回路２６１Ｂには、Ｍキーホルダ２５１Ｂから、ユーザマテン２０２Ｂの機器固有のＭキーが与えられる。Ｍキーホルダ２５１Ｂから読み出されたＭキーに基づいて、Ｃキーと、Ｃキーで暗号化されたコンテンツのデータが暗号化される。したがって、Ｍキー暗号化回路２６１Ｂからは、Ｍキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータが出力される。Ｍキー暗号化回路２６１Ｂから出力されるＭキーで暗号化されたＣキーと、Ｃキーで暗号化され更にＭキーで暗号化されたコンテンツのデータは、キー出力端子ＲＫＥＹ＿ＯＵＴ及びデータ出力端子ＲＤＡＴＡ＿ＯＵＴから各々出力され、ユーザマシン２０２Ｂのストレージデバイス２２０Ｂに記憶保存される。

このように、Ｔキーを用いると、ユーサマシン２０２Ａからユーザマシン２０２Ｂにデータを移動する際に、ユーサマシン２０２Ａからユーザマシン２０２Ｂに送信されるＣキー及びＣキーで暗号化されたコンテンツのデータは、更にＴキーで暗号化される。このため、外部に暗号化キーとしてのＣキーが漏れることがなく、コンテンツのデータの保護が図れる。

５．ＤＡコードを用いたシステム

上述したように、Ｔキーをデータ配信テステムに導入すると、或る機器としてのユーザマシンと他の機器としてのユーザマシンとの間にデー

タを移動させる際のデータ保護を図ることができる。しかしながら、上述したように、Ｔキーを導入したとしても、同一の機器内でデータを移動することは可能である。例えば、Ｃキーを同一のユーザマシン内の別の場所、例えば別な記憶部に一時的に保存しておいてから、コンテンツのデータの移動を行ない、その後に、Ｃキーを元に戻すようなことを行なうと、コンテンツデータの移動によってＣキーは消去されてしまうが、Ｃキーが別な場所に別途保存されているので、保存されているＣキーを用いれば、コンテンツのデータが不正に複製されてしまう。

そこで、Ｃキーに、時間と共に動的に変化するコード（ＤＡコードと称する）を付加して、Ｃキーに時間的に変化する要素を持たせることが考えられる。以下、時間的に変化する要素を有するＣキーを用いたデータ配信システムについて第９図以下に説明する。

つまり、第９図において、ユーザマシン３０２は、Ｃキー保存メモリ３３０以外は前述した第３図に示したユーザマシン１０２と同様に、ストレージデバイス３２０、暗号化／復号化処理部３２１、入力部３２２、ユーザインターフェース３２３、マシン処理マネージャ３２４、通信マネージャ３２５、カードリーダ／ライタ３２７から構成される。カードリーダ／ライタ３２７には、前述した第３図に示したカード１２６と同様のカード３２６が装着される。

このようなユーザマシン３０２で、例えばストレージデバイス３２０からＣキーを読み出し、ストレージデバイス３２０から読み出されたこのＣキーをＣキー保存メモリ３３０に保存しておいてから、ストレージデバイス３２０のコンテンツのデータを他の機器としての他のユーザマシンに移動したとする。この場合、コンテンツのデータの移動が終了すると、ストレージデバイス３２０のＣキーは消されるが、Ｃキー保存メモリ３３０にＣキーを退避させているので、メモリ３３０のＣキーは消

去されない。その後、Ｃキー保存メモリ３３０からのＣキーをストレージデバイス３２０に戻せば、ストレージデバイス３２０にコンテンツのデータが残っていれば、他のユーザマシンに移動したはずのコンテンツのデータを復号できてしまう。更に、ストレージデバイス３２０にコンテンツデータが無くても、Ｃキーがあれば、前述したようにコンテンツサーバ１からコンテンツのデータの再送が要求を行なうことができ、コンテンツデータの不正使用が可能となる。

そこで、本データ配信システムでは、第１０図に示すように、Ｃキーに、時間と共に動的に変化するＤＡコードが付加される。このＤＡコードとしては、タイムコードや乱数が用いられる。このように、ＣキーにＤＡコードを付加することにより、上述したようなコンテンツのデータの不正利用を防止することができる。

第１１図は、第１０図に示したＤＡコードが付加されたＣキーを扱うための暗号化／復号化処理部３２１の構成を示すものである。暗号化／復号化処理部３２１には、第７図に示した暗号化／復号化処理部２２１Ａ、２２１Ｂと同様に、Ｍキーホルダ３５１と、ＭＩＤホルダ３５２と、Ｍキー復号化回路３５３と、コントローラ３５４と、Ｃキー取り込み回路３５５と、Ｃキー復号化回路３５６と、Ｔキー暗号化回路３５７と、Ｔキー生成回路３５８、３５９と、Ｔキー復号化回路３６０と、Ｍキー暗号化回路３６１とが設けられると共に、ＤＡコード管理回路３６２とが設けられる。

ＤＡコード管理回路３６２は、Ｃキーに付加するＤＡコードの管理を行なうものである。すなわち、ＤＡコード管理回路３６２は、所定時間毎にストレージデバイス３２０からのＣキーを呼び出しを行なう。Ｃキーが呼び出されると、ＣキーのＤＡコードのチェックを行い、ＤＡコードが正しければ、ＤＡコートの更新処理を行なう。

なお、ストレージデバイス３２０には、Ｍキーで暗号化されたＣキーが保存されている。したがって、このＭキーで暗号化されたＣキーは、先ず、キー入力端子ＫＥＹ＿ＩＮから、Ｍキー復号化回路３５３に送られて、Ｍキーに基づいて施されている暗号化の復号処理が行なわれる。Ｍキー復号化回路３５３から、復号されたＣキーが出力され、このＣキーは、ＤＡコード管理回路３６２に送られる。

ＤＡコード管理回路３６２は、復号化回路３５３から供給されるＣキーのＤＡコードを所定時間毎に検出して正しく更新されているＤＡコードがＣキーに付加されているか否かを判断し、Ｃキーに付加されている正しく更新されているＤＡコードなら、ＤＡコードの更新を行なう。このＤＡコードが更新されたＣキーをＭキー暗号化回路３６１に供給して再びＭキーに基づいて暗号化処理を行なって、再び、ストレージデバイス３２０に保存する。Ｃキーに付加されているＤＡコードのタイムコートである場合にはタイムコードが所定の規則に従って変化しているものであるか否かを判断することによって行なわれるようにしても良く、後述するステップＳ１３で用いている手法に基づいて判断しても良い。

第１２図は、ＤＡコード管理回路３６２の処理を示すフローチャートである。第１２図において、例えばコントローラ３５４又はＤＡコード管理回路３６２のタイマ機能によって所定時間経過したか否かが判断され（ステップＳ１１）、所定時間経過したら、ストレージデバイス３２０よりＣキーが読み出されて復号化回路３５３で復号され、復号されたＣキーに付加されているＤＡコードが検出される（ステップＳ１２）。ストレージデバイス３２０より読み出されたＤＡコードが正しく更新されているＤＡコードであるか否かが判断される（ステップＳ１３）。このステップＳ１３でＤＡコードが正しく更新されているか否かは、暗号化／復号化処理部３１内に保持しているＤＡコードとストレージデバイ

ス３２０から読み出されたＤＡコードが一致しているか否かにより判断できる。ステップＳ１３で正しく更新されているＤＡコードであると判断されると、このＤＡコードが次のＤＡコードに更新され、そして、この更新されたＤＡコードが付加されたＣキーは、再び、Ｍキー暗号化回路３６１によってＭキーに基づいて暗号化処理が施されてストレージデバイス３２０に戻される（ステップＳ１４）。

ステップＳ１３で、検出されたＤＡコードが正しく更新されているＤＡコードではないと判断されたら、ストレージデバイス３２０のＣキーを消去し、又は、Ｃキーに不正利用を示すコードを付加して、ＤＡコードが正しく更新されていないと判断されたＣキーに対応するそのコンテンツのデータの利用が禁止される（ステップＳ１５）。

このように、ストレージデバイス３２０のＣキーが正常に扱われている場合には、ＤＡコード管理回路３６２で、Ｃキーに付加されるＤＡコードが所定の時間毎に絶えず更新され、更新されたＤＡコードが付加されたＣキーがストレージデバイス３２０に保存される。

例えば、Ｃキーを第９図におけるＣキー保存メモリ３３０に保存しておいたような場合には、Ｃキー保存メモリ３３０に保存されているＣキーのＤＡコードが上述のように更新されないので、ＤＡコード管理回路３６２で、ＤＡコードが正しくないと判断される。その結果、前述したようにＣキーを一旦メモリ３３０に保存しておいてコンテンツのデータの移動を行ない、移動後にメモリ３３０に保存されているＣコードを用いてコンテンツのデータの不正利用を行なうことを防止できる。

上述したように、動的に変化するＤＡコードを使うと、ある期間再生を禁止／許可することができるようになる。これを利用すると、コンテンツを所定の期間貸し出したり、コンテンツの利用に試用期間を設定したりすることができる。

第１３図は、上述したような動的に変化するＤＡコードを有するＣキーを用いて所定期間だけコンテンツのデータを再生可能に設定する場合の処理を示すフローチャートである。なお、第１３図に示す場合、ＤＡコードとしては、タイムコードが用いられる。このＣキーのＤＡコードには、更に、期限情報が付加される。

第１３図において、上述したステップＳ１１と同様にして所定時間経過したか否かが判断され（ステップＳ２１）、所定時間経過したら、ストレージデバイス３２０に保存されているＣキーが呼び出される。上述したステップＳ１２と同様に、このＣキーに付加されているＤＡコードが検出される（ステップＳ２２）。ＤＡコードが正しく更新されているか否かが判断される（ステップＳ２３）。ステップＳ２３で正しく更新されているＤＡコードであると判断されると、このＤＡコードが次のＤＡコードにＤＡコード管理回路３６２で更新される（ステップＳ２４）。この更新されたＤＡコードに付加されている期限情報とコンテンツデータの使用期限を示し、ＤＡコード管理コードに保持されている期限情報とが比較され、Ｃキーが使用期限超過か否かが判断される（ステップＳ２５）。Ｃキーが使用期限超過でなければ、この更新されたＤＡコードが付加されたＣキーがストレージデバイス３２０に戻され（ステップＳ２６）、ステップＳ２１リターンされる。

ステップＳ２３で、ストレージデバイス３２０から呼び出されたＤＡコードが正しく更新されているものではないと判断されたら、ストレージデバイス３２０からＣキーが削除され、又は、Ｃキーに不正使用を示すコードが付加されて、ＤＡコードが正しく更新されていないと判断されたＣキーに対応するコンテンツのデータの利用不可能とされる。（ステップＳ２６）。ステップＳ２５で、Ｃキーの使用期間超過であると判断されると、ステップＳ２６に移行し、ストレージデバイス３２０から

Ｃキーが削除され、又は、Ｃキーに不正使用を示すコードが付加されて、上述と同様に使用期限超過と判断されたＣキーに対応するコンテンツのデータの利用不可能とされる。

このようにして、ＤＡコードを用いて、ある期間だけコンテンツのデータの再生を禁止又は許可したりすることができる。これにより、試用期間を設けて、ユーザがコンテンツのデータを再生させるようなことができる。更に、一方のユーザマシンから他方のユーザマシンにコンテンツのデータを移動する場合に、一方のユーザマシンのＣキーをＤＡコードにより所定の期限まで再生禁止とし、他方のユーザマシンのＣキーをその期間のみ再生可能とすると、一方のマシンから他方のマシンに所定の期間だけコンテンツのデータを貸すような制御が行なえる。

この発明によれば、コンテンツサーバに保存されるコンテンツは、Ｃキーで暗号化されている。このように、Ｃキーを設けることにより、コンテンツを移動したり、再送を要求したりできる。また、送られてきたＣキーと同一のＣキーがストレージデバイスに保存さているか否かを判断することにより、再送か否かを判断して、適切な課金を行なったり、Ｃキーにランクを付けてコンテンツ毎に料金を変えて課金を行なうようなことができる。

また、この発明によれば、Ｃキーに、時間と共に動的に変化するＤＡコードが付加される。このようなＤＡコードを付加することで、Ｃキーを退避させておいて、コンテンツを不正利用するようなことが防止できる。また、この時間と共に動的に変化するＤＡコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

産業上の利用可能性

以上のように、この発明にかかるデータ配信装置及びデータ配信用の端末装置は、例えば、複数の音楽データが蓄積されるコンテンツサーバと、このコンテンツサーバに蓄積されたコンテンツから所望のコンテンツが配信されるユーザマシンとからなる情報配信システムに用いて好適である。

請　求　の　範　囲

1．機器固有の第1の識別データと上記第1の識別データと対応する第2の識別データとが記憶されている第1の記憶部と、

上記第1の記憶部から読み出された上記第1の識別データとともにデータの配信要求データを送信するとともに送信されてきたデータを受信する第1の送受信部と、

上記データ送受信部によって受信されたデータを蓄える第1のデータ記憶部と、

上記第1のデータ記憶部から読み出されたデータを上記第1の記憶部に記憶されている上記第2の識別データに基づいて復号化処理を施す第1の信号処理部と、

上記第1の送受信部によって受信されたデータを上記第1のデータ記憶部に記憶させる動作を行うとともに上記第1のデータ記憶部から読み出されたデータの上記第1の信号処理部による復号化処理動作を制御する第1の制御部と、

上記第1の送受信部から送信されてきた上記第1の識別データと上記配信要求データを受信するとともにデータの送信を行う第2の送受信部と、

複数のデータが記憶され、上記配信要求データに対応するデータを出力する第2のデータ記憶部と、

上記送信されてきた第1の識別データに対応する第2の識別データが記憶されている第2の記憶部と、

上記第2のデータ記憶部から出力されたデータに上記第2の記憶部から読み出された第2の識別データに基づいて暗号化処理を施す第2の信号処理部と、

上記送信されてきた配信要求データと上記第1の識別データに基づいて上記第2の記憶部から上記第2の識別データの読み出し制御を行うとともに上記配信要求データに基づいて上記第2のデータ記憶部からデータの読み出し制御を行う第2の制御部とを備え、

上記第2の送受信部を介して送信されてきた上記第2の識別データに基づいて暗号化されたデータを上記第1の信号処理部によって復号するデータ配信装置。

2．上記第2の制御部は、上記第1の送受信部から課金情報が上記第2の送受信部に送信され、上記送信されてきた課金情報に基づいて上記第2の記憶部からの上記第2の識別データの読み出しを制御する請求の範囲第1項記載のデータ配信装置。

3．上記装置は、更に上記第2のデータ記憶部に書き込まれるデータに暗号化データに基づいて暗号化処理を施す暗号化処理手段を備え、上記暗号化処理手段によって暗号化されたデータは上記第2のデータ記憶部に書き込まれるとともに、上記配信要求データに基づいてデータを上記第2のデータ記憶部から読み出して上記第2の送受信部から上記第1の送受信部に送信する際に上記暗号化データを上記第2の信号処理部によって上記第2の識別データによって暗号化して上記第2のデータ記憶部から読み出されたデータとともに送信する請求の範囲第1項記載のデータ配信装置。

4．上記第1の信号処理部は、上記第2の送受信部から送信されてきたデータと上記暗号化データを上記第1の記憶部に記憶されている上記第2の識別データによって復号するとともに、復号された暗号化データに基づいて復号されたデータに上記暗号化データによって施されている暗号の復号処理を行う請求の範囲第3項記載のデータ配信装置。

5．上記第1の制御部は、上記暗号化データに基づいて課金処理を行う

請求の範囲第３項記載のデータ配信装置。

６．上記暗号化データは動的に変化でするデータ部を有し、上記第１の制御部は、上記第１のデータ記憶部に記憶されている上記第２の送受信部からデータとともに送信されてきた上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲第４項記載のデータ配信装置。

７．上記第１の制御部は、上記動的に変化するデータ部の判別結果に基づいて上記第１のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第６項記載のデータ配信装置。

８．上記第１の制御部は、上記動的に変化するデータ部の判別結果が上記暗号化データが正しくないときには少なくとも上記第１のデータ記憶部からのデータの読み出し動作を禁止する請求の範囲第７項記載のデータ配信装置。

９．上記暗号化データは時間的に変化するデータ部を有し、上記第１の制御部は、上記第１のデータ記憶部に記憶されている上記第２の送受信部からデータとともに送信されてきた上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲第４項記載のデータ配信装置。

１０．上記第１の制御部は、上記時間的に変化するデータ部の判別結果に基づいて上記第１のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第９項記載のデータ配信装置。

１１．上記第１の制御部は、上記時間的に変化するデータ部の判別結果が所定時間を過ぎているときには少なくとも上記記憶部からのデータの読み出し動作を禁止する請求の範囲第１０項記載のデータ配信装置。

１２．上記装置は、更に上記第１のデータ記憶部に記憶されているデータを移動するときに上記第１の信号処理部によって復号化されたデータ

に更にデータを移動する先の第1の識別データに基づいて暗号化処理を施す更なる信号処理部を備えている請求の範囲第4項記載のデータ配信装置。

１３．上記第１の制御部は、上記第１のデータ記憶部に記憶されているデータの移動が終了した時点で上記第１のデータ記憶部に記憶されている上記暗号化データを削除する請求の範囲第１２項記載のデータ配信装置。

１４．機器固有の第１の識別データと上記第１の識別データと対応する第２の識別データとが記憶されている第１の記憶部と、上記第１の記憶部から読み出された上記第１の識別データとともにデータの配信要求データを送信するとともに送信されてきたデータを受信する第１のデータ送受信部と、上記データ送受信部によって受信されたデータを蓄える第１のデータ記憶部と、上記第１のデータ記憶部から読み出されたデータを上記第１の記憶部に記憶されている上記第２の識別データに基づいて復号化処理を施す第１の信号処理部と、上記第１の送受信部によって受信されたデータを上記第１のデータ記憶部に記憶させる動作を行うとともに上記第１のデータ記憶部から読み出されたデータの上記第１の信号処理部による復号化処理動作を制御する第１の制御部とを有する少なくともひとつの端末機器部と、

上記端末機器部と伝送路を介して接続され、上記第１の送受信部から送信されてきた上記第１の識別データと上記配信要求データを受信するとともにデータの送信を行う第２の送受信部と、複数のデータが記憶され、上記配信要求データに対応するデータを出力する第２のデータ記憶部と、上記送信されてきた第１の識別データに対応する第２の識別データが記憶されている第２の記憶部と、上記第２のデータ記憶部から出力されたデータに上記第２の記憶部から読み出された第２の識別データに

基づいて暗号化処理を施す第２の信号処理部と、上記送信されてきた配信要求データと上記第１の識別データに基づいて上記第２の記憶部から上記第２の識別データの読み出し制御を行うとともに上記配信要求データに基づいて上記第２のデータ記憶部からデータの読み出し制御を行う第２の制御部とを有するサーバ装置部とを備え、

上記第２の送受信部を介して送信されてきた上記第２の識別データに基づいて暗号化されたデータを上記第１の信号処理部によって復号するデータ配信装置。

１５．上記第２の制御部は、上記第１の送受信部から課金情報が上記第２の送受信部に送信され、上記送信されてきた課金情報に基づいて上記第２の記憶部からの上記第２の識別データの読み出しを制御する請求の範囲第１４項記載のデータ配信装置。

１６．上記装置は、更に上記第２のデータ記憶部に書き込まれるデータに暗号化データに基づいて暗号化処理を施す暗号化処理手段を備え、上記暗号化処理手段によって暗号化されたデータは上記第２のデータ記憶部に書き込まれるとともに、上記配信要求データに基づいてデータを上記第２のデータ記憶部から読み出して上記第２の送受信部から上記第１の送受信部に送信する際に上記暗号化データを上記第２の信号処理部によって上記第２の識別データによって暗号化して上記第２のデータ記憶部から読み出されたデータとともに送信する請求の範囲第１４項記載のデータ配信装置。

１７．上記第１の信号処理部は、上記第２の送受信部から送信されてきたデータと上記暗号化データを上記第１の記憶部に記憶されている上記第２の識別データによって復号するとともに、復号された暗号化データに基づいて復号されたデータに上記暗号化データによって施されている暗号の復号処理を行う請求の範囲第１６項記載のデータ配信装置。

１８．上記第１の制御部は、上記暗号化データに基づいて課金処理を行う請求の範囲第１６項記載のデータ配信装置。

１９．上記暗号化データは動的に変化するデータ部を有し、上記第１の制御部は、上記第１のデータ記憶部に記憶されている上記第２の送受信部からデータとともに送信されてきた上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲１６項記載のデータ配信装置。

２０．上記第１の制御部は、上記動的に変化するデータ部の判別結果に基づいて上記第１のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第１９項記載のデータ配信装置。

２１．上記第１の制御部は、上記動的に変化するデータ部の判別結果が上記暗号化データが正しくないときには少なくとも上記第１のデータ記憶部からのデータ読み出し動作を禁止する請求の範囲第２０項記載のデータ配信装置。

２２．上記暗号化データは時間的に変化するデータ部を有し、上記第１の制御部は、上記第１のデータ記憶部に記憶されている上記第２の送受信部からデータとともに送信されてきた上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲１６項記載のデータ配信装置。

２３．上記第１の制御部は、上記時間的に変化するデータ部の判別結果に基づいて上記第１のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第２２項記載のデータ配信装置。

２４．上記第１の制御装置は、上記時間的に変化するデータ部の判別結果が所定時間を過ぎているときには少なくとも上記記憶部からのデータ読み出し動作を禁止する請求の範囲第２３項記載のデータ配信装置。

２５．上記装置は、更に上記第１のデータ記憶部に記憶されているデー

タを他の端末機器部に移動するときに上記第１の信号処理部によって復号化されたデータに更にデータを移動する先の上記他の端末機器部の第１の識別データに基づいて暗号化処理を施す更なる信号処理部を備えている請求の範囲第１６項記載のデータ配信装置。

２６．上記第１の制御部は、上記第１のデータ記憶部に記憶されているデータの移動が終了した時点で上記第１のデータ記憶部に記憶されている上記暗号化データを削除する請求の範囲第２５項記載のデータ配信装置。

２７．装置固有の第１の識別データと上記第１の識別データと対応する第２の識別データとが記憶されている記憶部と、

上記記憶部から読み出された上記第１の識別データとともにデータの配信要求データを送信するとともに上記第２の識別データによって暗号化されて送信されてきたデータを受信するデータ送受信部と、

上記データ送受信部によって受信された上記第２の識別データに基づいて暗号化されたデータを蓄えるデータ記憶部と、

上記データ記憶部から読み出されたデータを上記記憶部に記憶されている上記第２の識別データに基づいて復号処理を施す信号処理部と、

上記送受信部によって受信されたデータを上記データ記憶部に記憶させる動作を行うとともに上記データ記憶部から読み出されたデータの上記信号処理部による復号化処理動作を制御する制御部とを備えているデータ配信用の端末装置。

２８．上記データ記憶部には、上記データ送受信部によって受信されたデータと当該データに施されている暗号化に元となる暗号化データが記憶されており、上記信号処理部は、上記データ記憶部から読み出されたデータを上記第１の記憶部に記憶されている上記第２の識別データによって復号するとともに、復号された暗号化データに基づいて復号された

データに上記暗号化データによって施されている暗号の復号処理を行う請求の範囲第２７項記載のデータ配信用の端末装置。

２９．上記第１の制御部は、上記暗号化データに基づいて課金処理を行う請求の範囲第２８項記載のデータ配信用の端末装置。

３０．上記暗号化データは動的に変化するデータ部を有し、上記の制御部は、上記のデータ記憶部にデータとともに記憶されている上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲２８項記載のデータ配信用の端末装置。

３１．上記制御部は、上記動的に変化するデータ部の判別結果に基づいて上記データ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲債３０項記載のデータ配信用の端末装置。

３２．上記制御部は、上記動的に変化するデータ部の判別結果が上記暗号化データが正しくないときには少なくとも上記データ記憶部からのデータの読み出し動作を禁止する請求の範囲第３１項記載のデータ配信用の端末装置。

３３．上記暗号化データは時間的に変化するデータ部を有し、上記制御部は、上記データ記憶部にデータとともに記憶されている上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲２８項記載のデータ配信用の端末装置。

３４．上記制御部は、上記時間的に変化するデータ部の判別結果に基づいて上記第１のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第３０項記載のデータ配信用の端末装置。

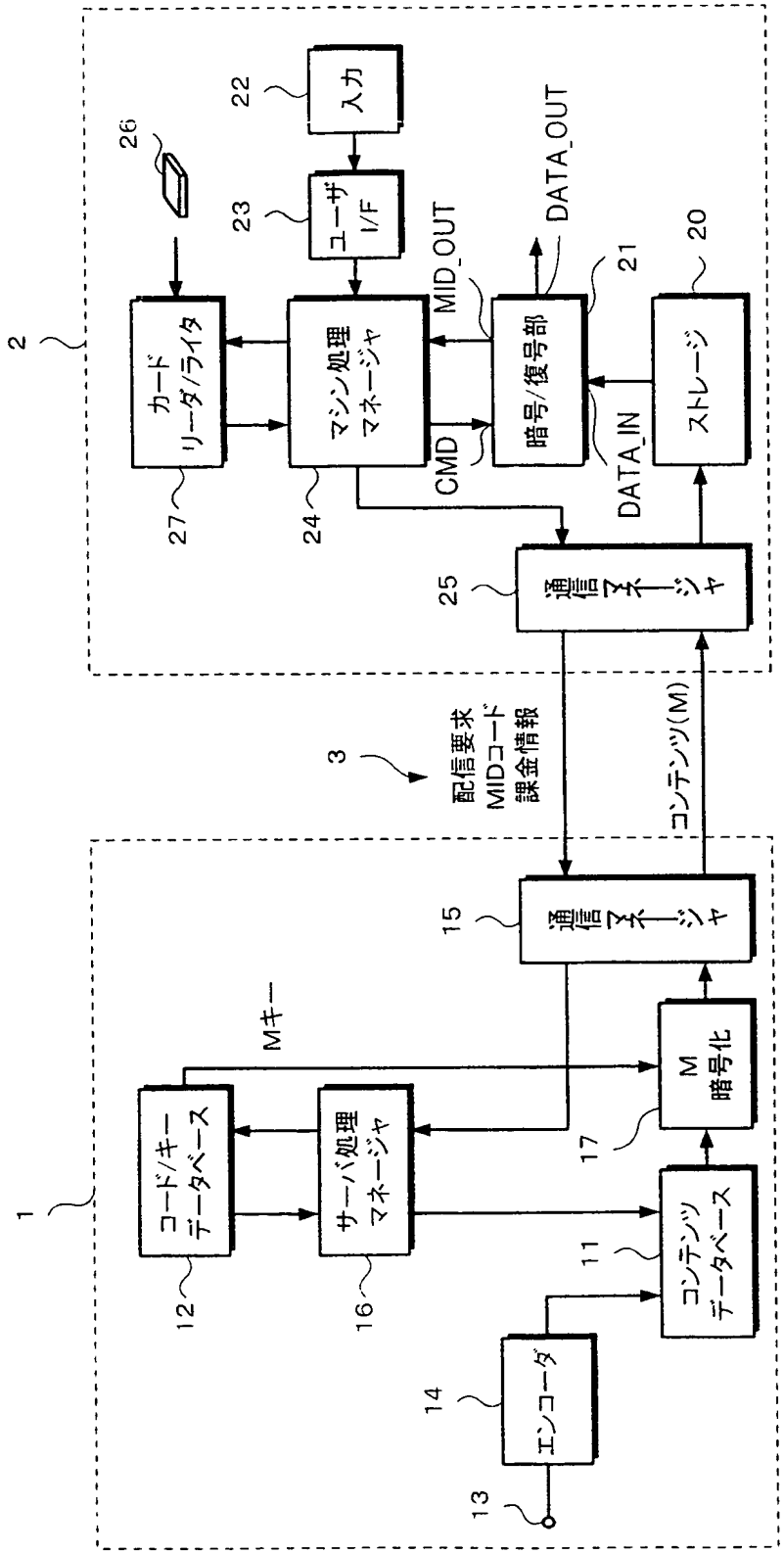
３５．上記制御部は、上記時間的に変化するデータ部の判別結果が所定時間を過ぎているときには少なくとも上記記憶部からのデータの読み出し動作を禁止する請求の範囲第３１項記載のデータ配信用端末装置。

３６．上記装置は、更に上記データ記憶部に記憶されているデータを移

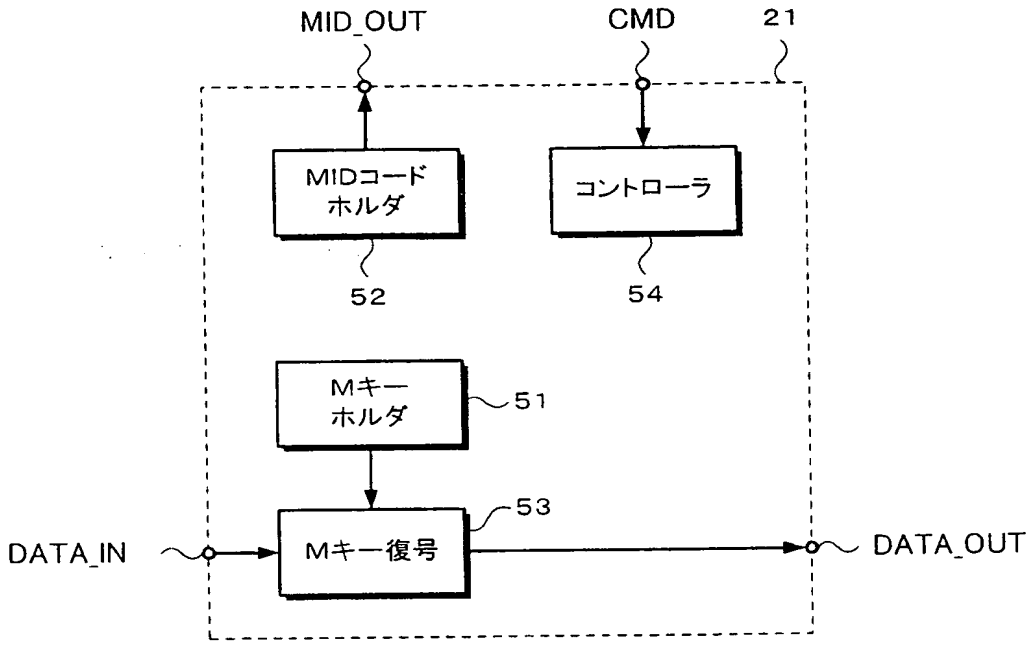
動するときに上記信号処理部によって復号化されたデータに更にデータを移動する先の第１の識別データに基づいて暗号化処理を施す更なる信号処理部を備えている請求の範囲第２８項記載のデータ配信用端末装置。

３７．上記制御部は、上記データ記憶部に記憶されているデータの移動が終了した時点で上記のデータ記憶部に記憶されている上記暗号化データを削除する請求の範囲第３３項記載のデータ配信用端末装置。

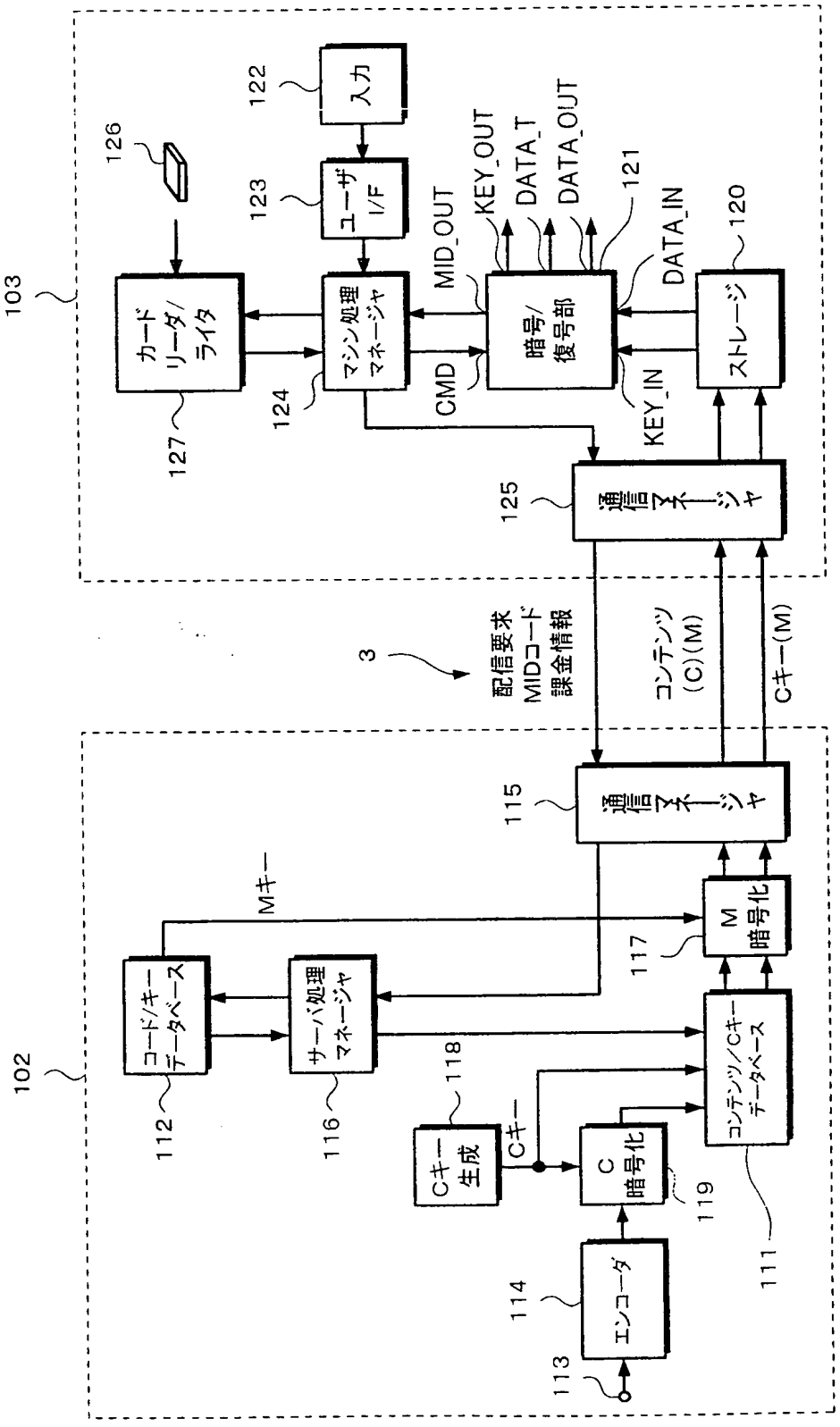
第1図


1
2
3
入力
ユーザ I/F
カード リーダ/ライタ
マシン処理 マネージャ
暗号/復号部
ストレージ
通信マネージャ
配信要求 MIDコード 課金情報
コンテンツ(M)
MID_OUT
DATA_OUT
CMD
DATA_IN
Mキー
コード/キー データベース
サーバ処理 マネージャ
M 暗号化
コンテンツ データベース
エンコーダ
11
12
13
14
15
16
17
20
21
22
23
24
25
26
27

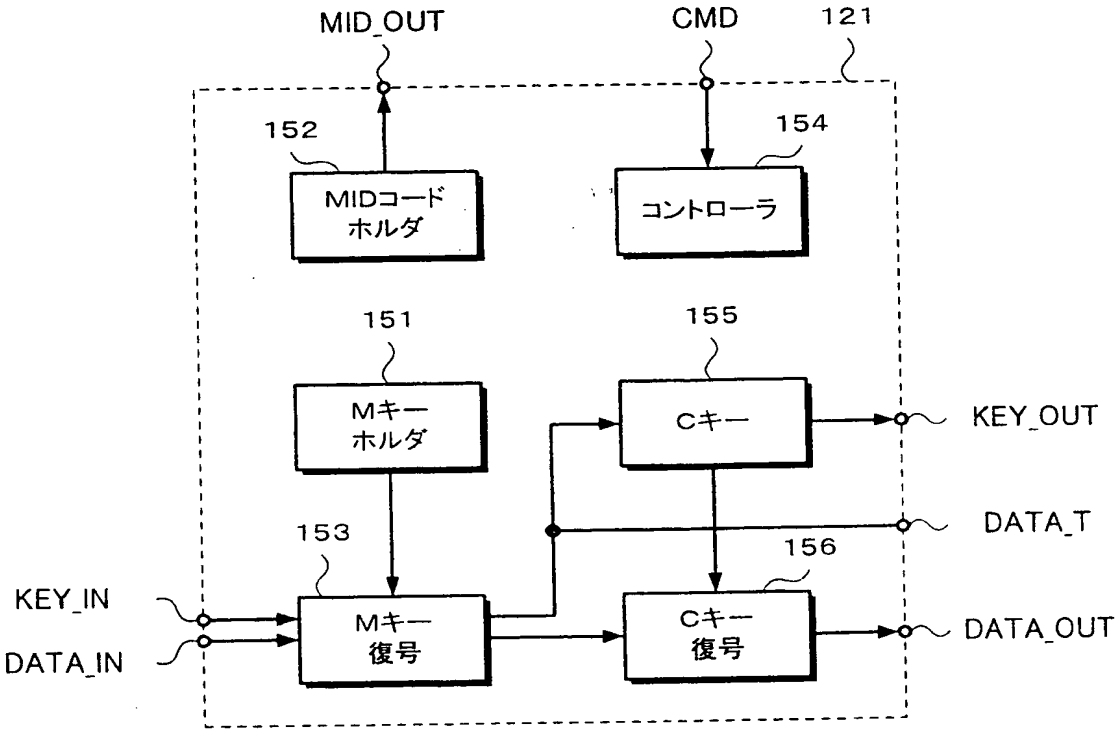
第２図


MID_OUT
CMD
21
MIDコード
ホルダ
コントローラ
52
54
Mキー
ホルダ
51
53
DATA_IN
Mキー復号
DATA_OUT

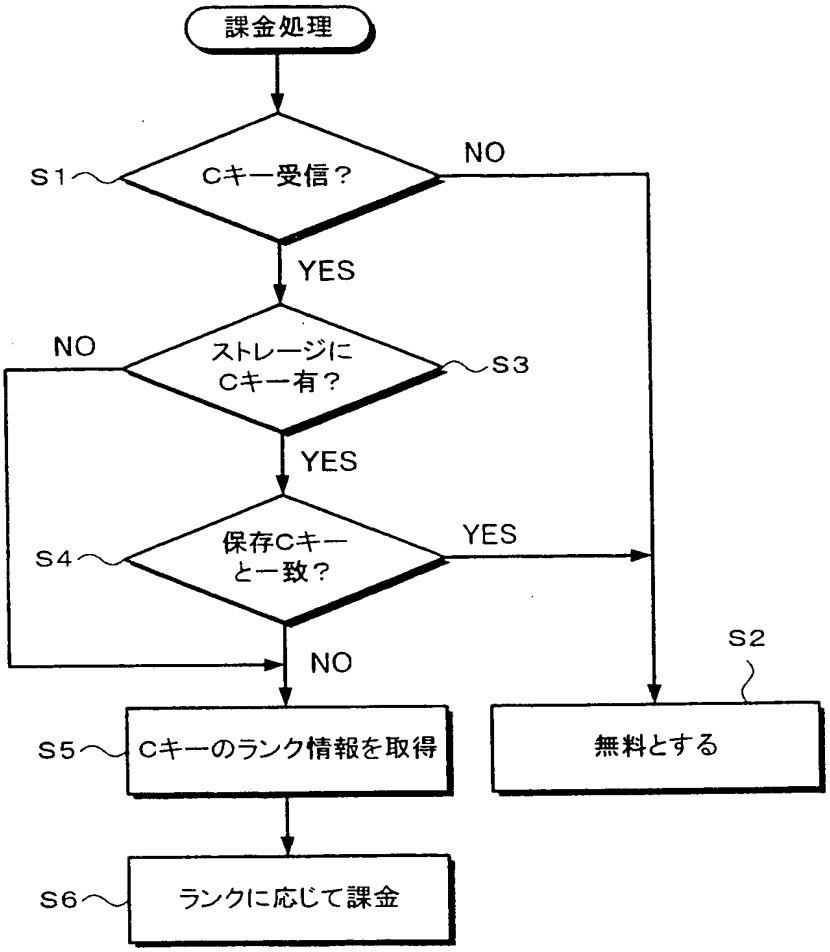
第3図


102
103
3
112
116
118
Cキー生成
Cキー
C暗号化
119
111
114
エンコーダ
113
コンテンツ/Cキーデータベース
M暗号化
117
115
通信マネージャ
Mキー
コード/キーデータベース
サーバ処理マネージャ
配信要求
MIDコード
課金情報
コンテンツ(C)(M)
Cキー(M)
125
通信マネージャ
127
カードリーダ/ライタ
126
124
マシン処理マネージャ
123
ユーザI/F
122
入力
CMD
MID_OUT
KEY_OUT
DATA_T
DATA_OUT
121
暗号/復号部
KEY_IN
DATA_IN
120
ストレージ

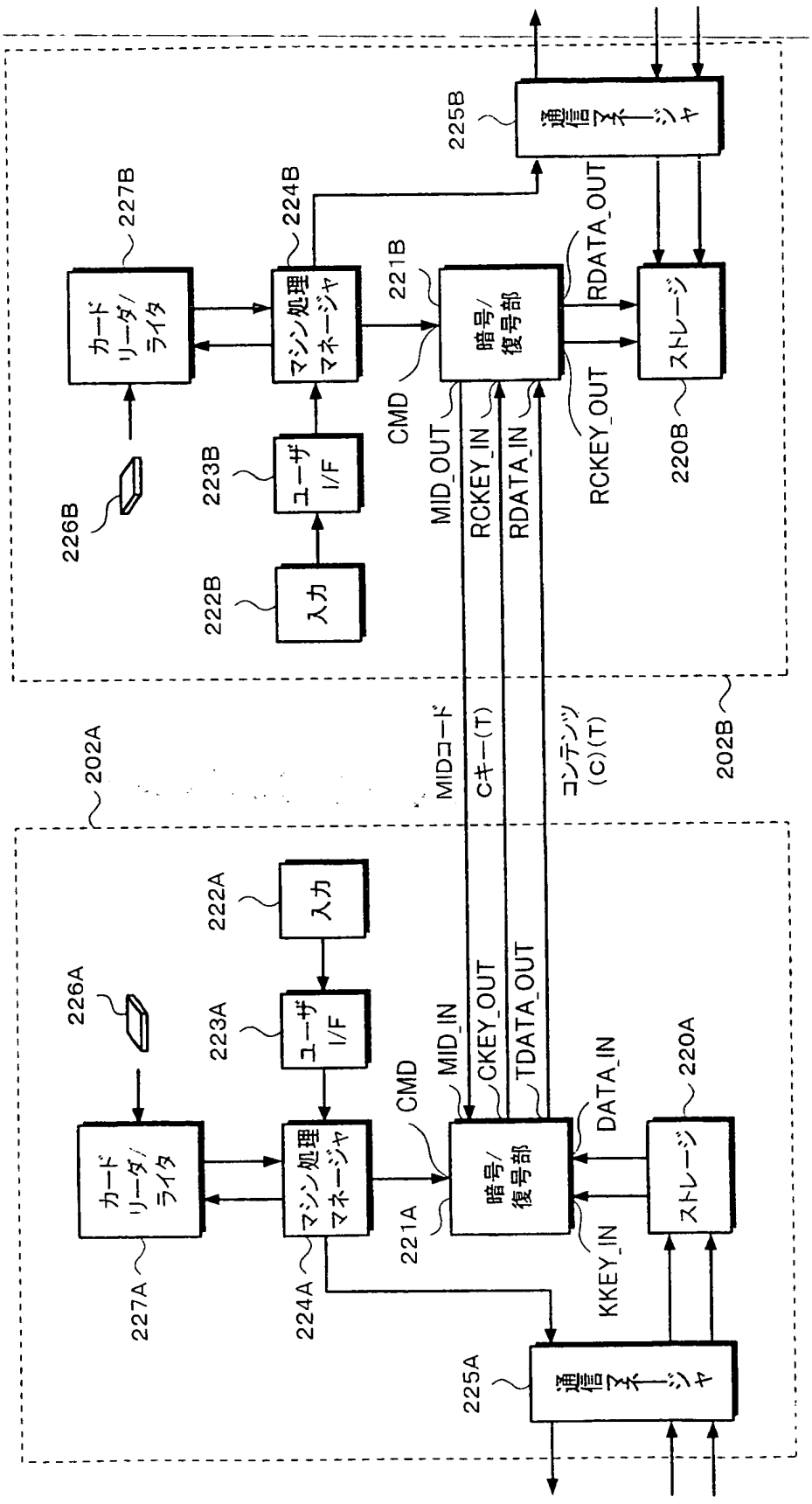
第４図


MID_OUT
CMD
121
152
154
MIDコード
ホルダ
コントローラ
151
155
Mキー
ホルダ
Cキー
KEY_OUT
DATA_T
153
156
KEY_IN
DATA_IN
Mキー
復号
Cキー
復号
DATA_OUT

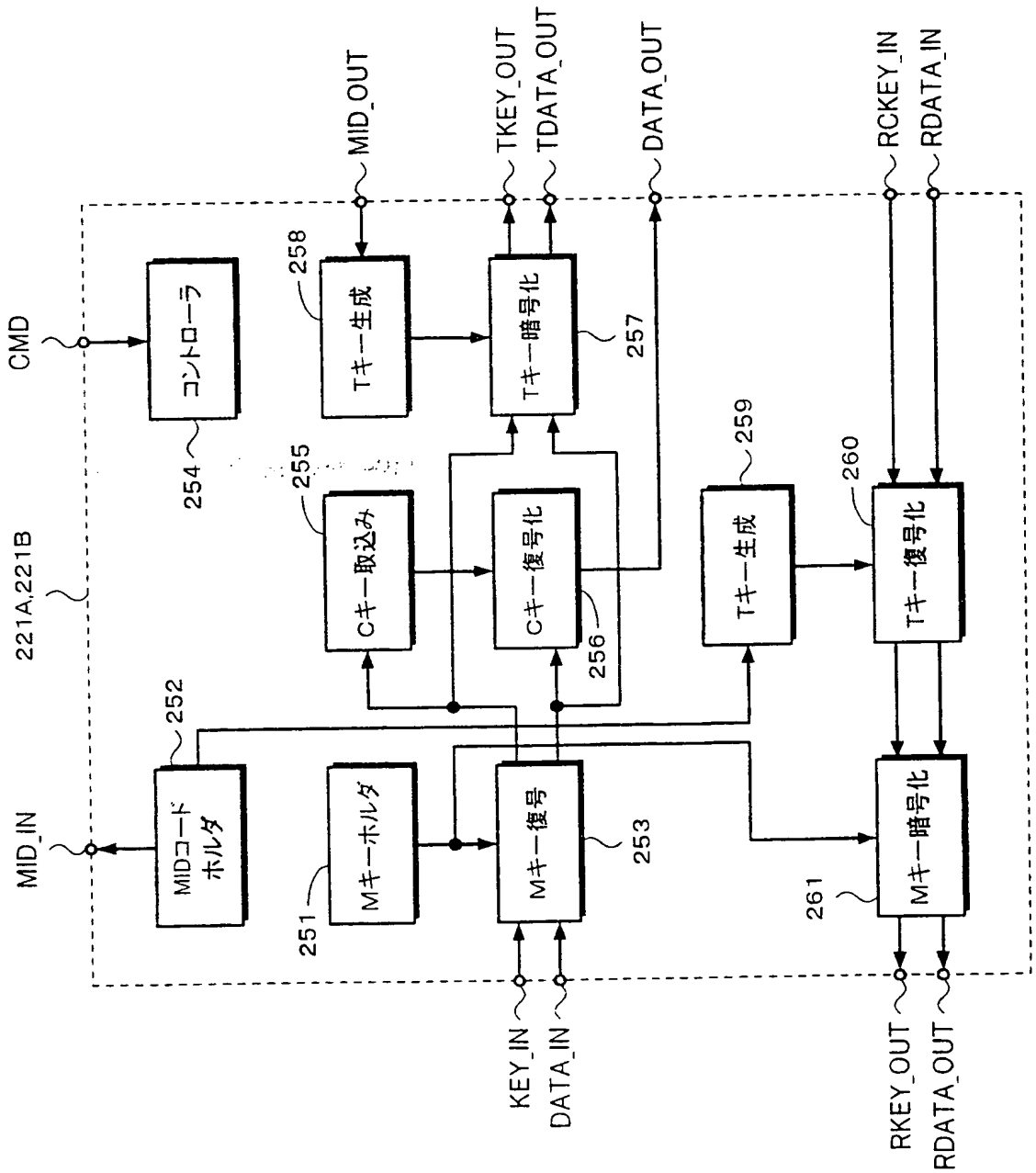
第５図


課金処理
S1
Cキー受信？
NO
YES
NO
ストレージに
Cキー有？
S3
YES
S4
保存Cキー
と一致？
YES
NO
S2
S5
Cキーのランク情報を取得
無料とする
S6
ランクに応じて課金

第6図

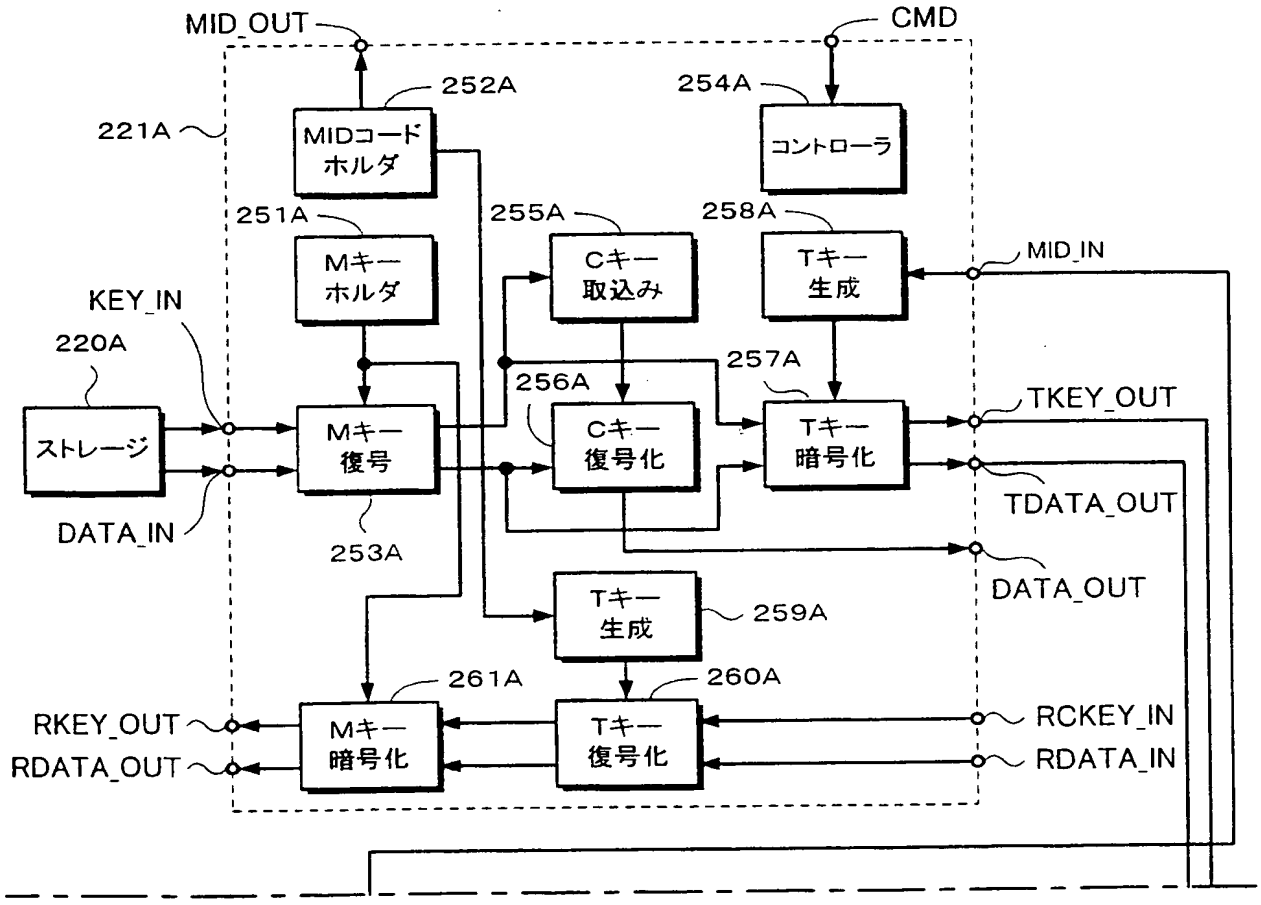

202A
202B
MIDコード
Cキー(T)
コンテンツ(C)(T)
225B
通信マネージャ
227B
カードリーダ/ライタ
224B
マシン処理マネージャ
221B
暗号/復号部
RDATA_OUT
ストレージ
CMD
MID_OUT
RCKEY_IN
RDATA_IN
RCKEY_OUT
220B
226B
223B
ユーザI/F
222B
入力
225A
通信マネージャ
227A
カードリーダ/ライタ
224A
マシン処理マネージャ
221A
暗号/復号部
DATA_IN
ストレージ
220A
CMD
MID_IN
CKEY_OUT
TDATA_OUT
KKEY_IN
226A
223A
ユーザI/F
222A
入力

第7図

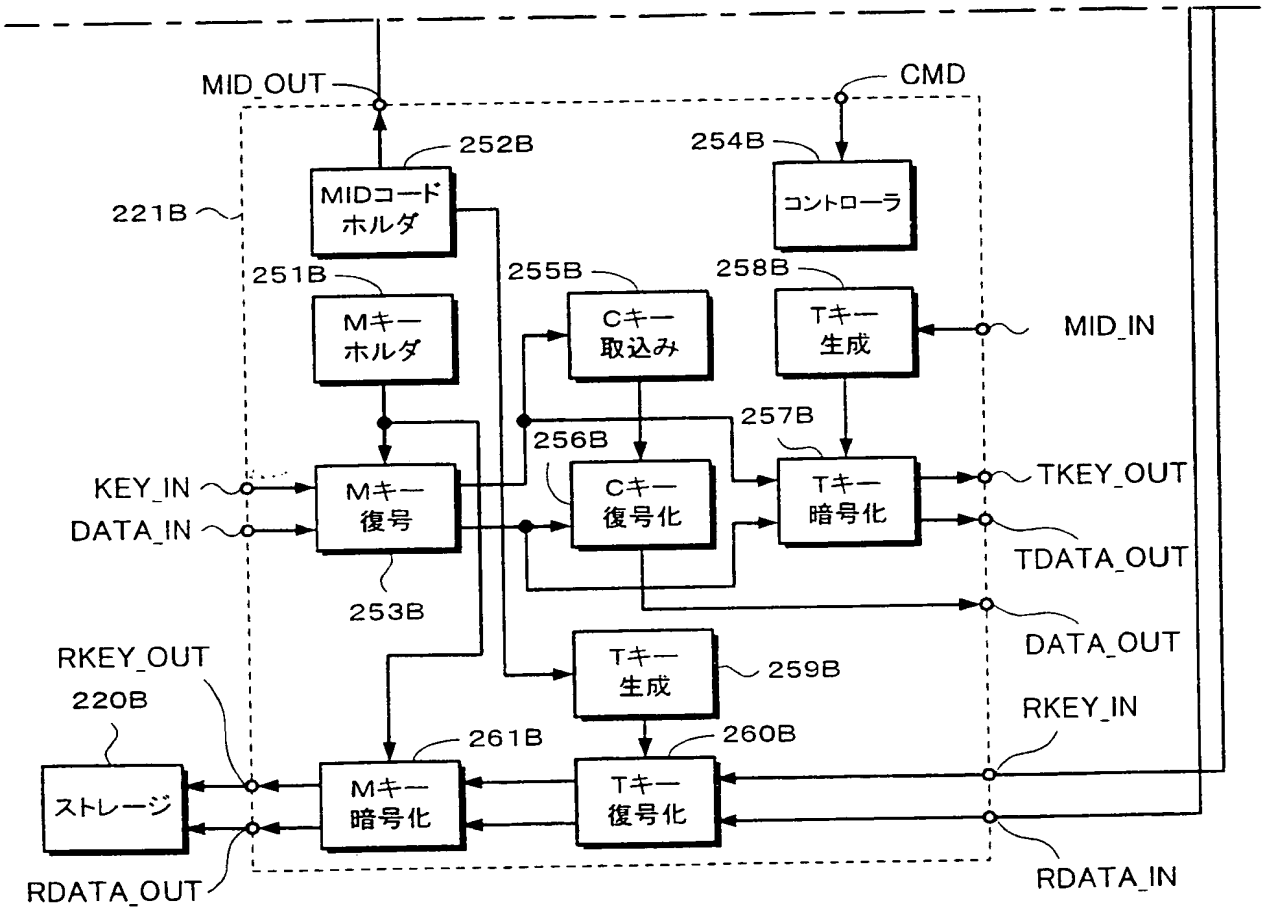

CMD
221A,221B
MID_IN
MIDコード ホルダ
252
コントローラ
254
Mキーホルダ
251
Mキー復号
253
Cキー取込み
255
Cキー復号化
256
Tキー生成
258
Tキー暗号化
257
Tキー生成
259
Tキー復号化
260
Mキー暗号化
261
MID_OUT
TKEY_OUT
TDATA_OUT
DATA_OUT
RCKEY_IN
RDATA_IN
KEY_IN
DATA_IN
RKEY_OUT
RDATA_OUT

第８図
第８図Ａ
第８図Ｂ

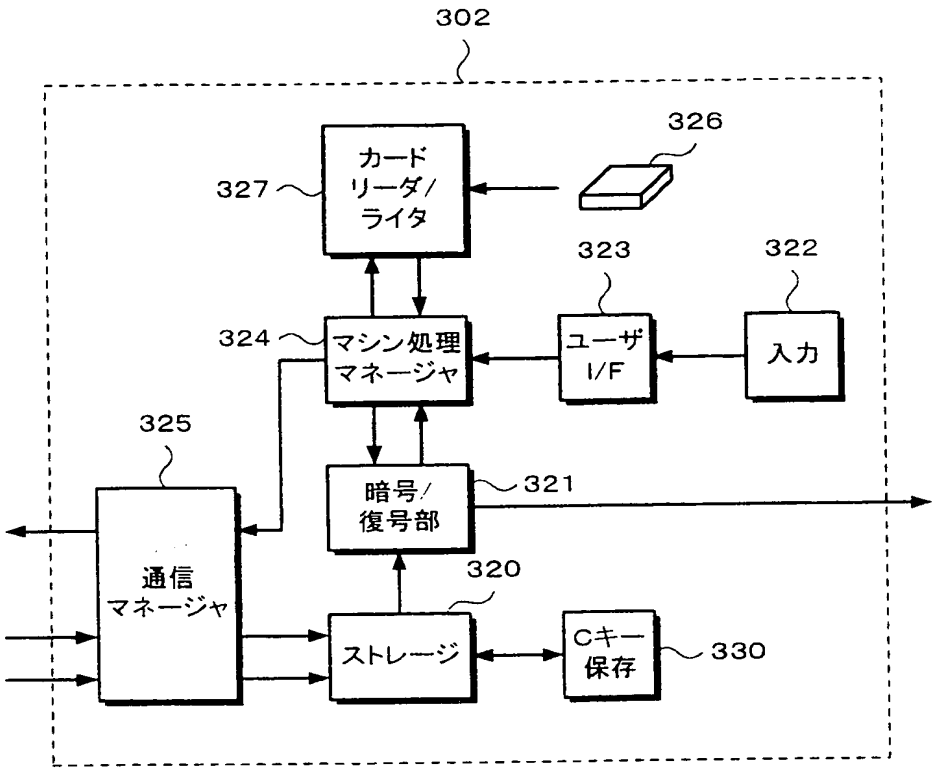
第８図Ａ



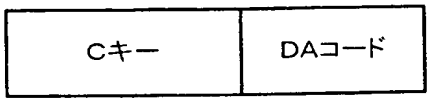
第８図Ｂ


MID_OUT
CMD
252B
254B
MIDコード
ホルダ
コントローラ
221B
251B
255B
258B
Mキー
ホルダ
Cキー
取込み
Tキー
生成
MID_IN
257B
256B
KEY_IN
DATA_IN
Mキー
復号
Cキー
復号化
Tキー
暗号化
TKEY_OUT
TDATA_OUT
253B
DATA_OUT
RKEY_OUT
Tキー
生成
259B
220B
RKEY_IN
261B
260B
ストレージ
Mキー
暗号化
Tキー
復号化
RDATA_OUT
RDATA_IN

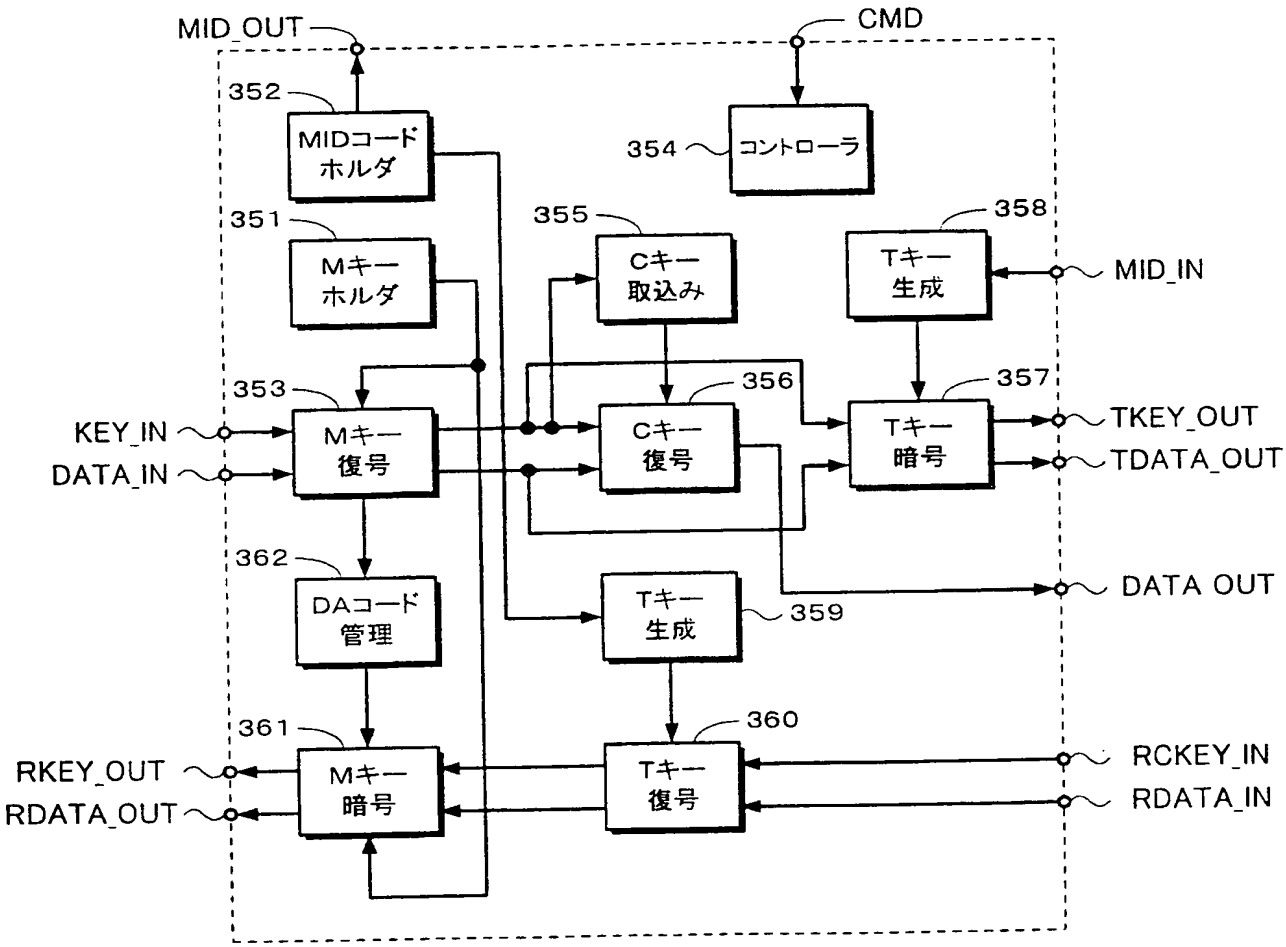
第９図


302
326
カード
リーダ/
ライタ
327
323
322
324
マシン処理
マネージャ
ユーザ
I/F
入力
325
暗号/
復号部
321
通信
マネージャ
320
ストレージ
Cキー
保存
330

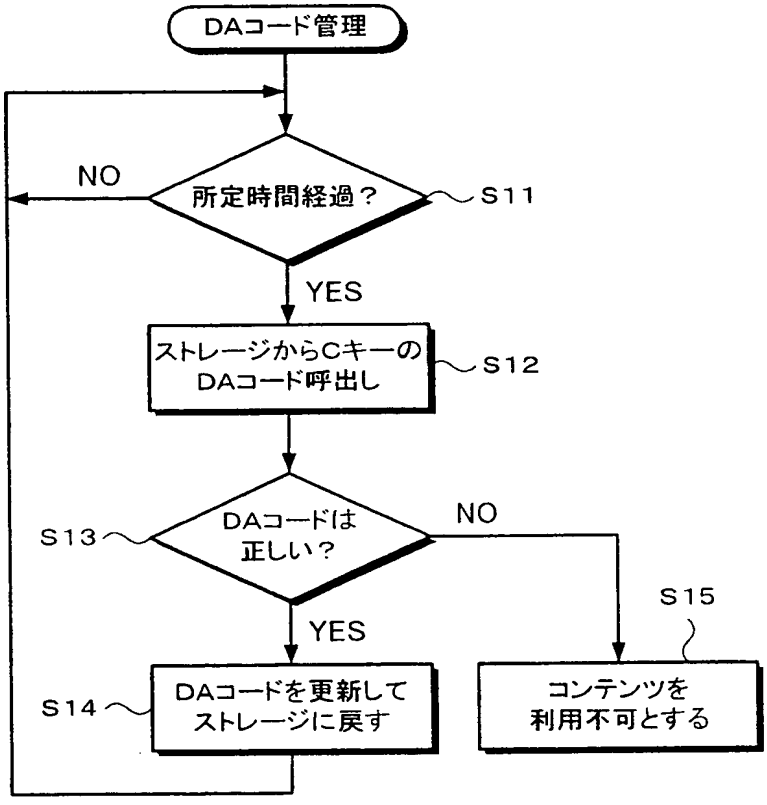
第１０図


Cキー
DAコード

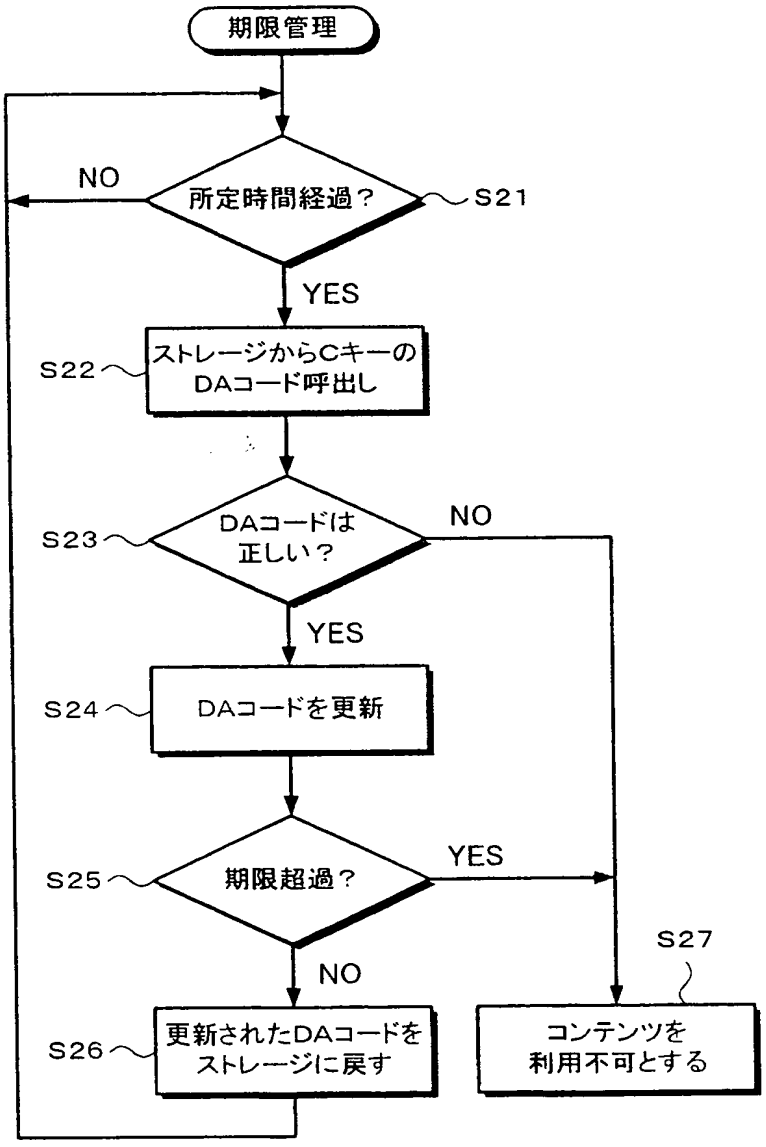
第１１図


MID_OUT
CMD
352
MIDコード
ホルダ
354
コントローラ
351
Mキー
ホルダ
355
Cキー
取込み
358
Tキー
生成
MID_IN
353
KEY_IN
DATA_IN
Mキー
復号
356
Cキー
復号
357
Tキー
暗号
TKEY_OUT
TDATA_OUT
362
DAコード
管理
Tキー
生成
359
DATA OUT
361
RKEY_OUT
RDATA_OUT
Mキー
暗号
360
Tキー
復号
RCKEY_IN
RDATA_IN

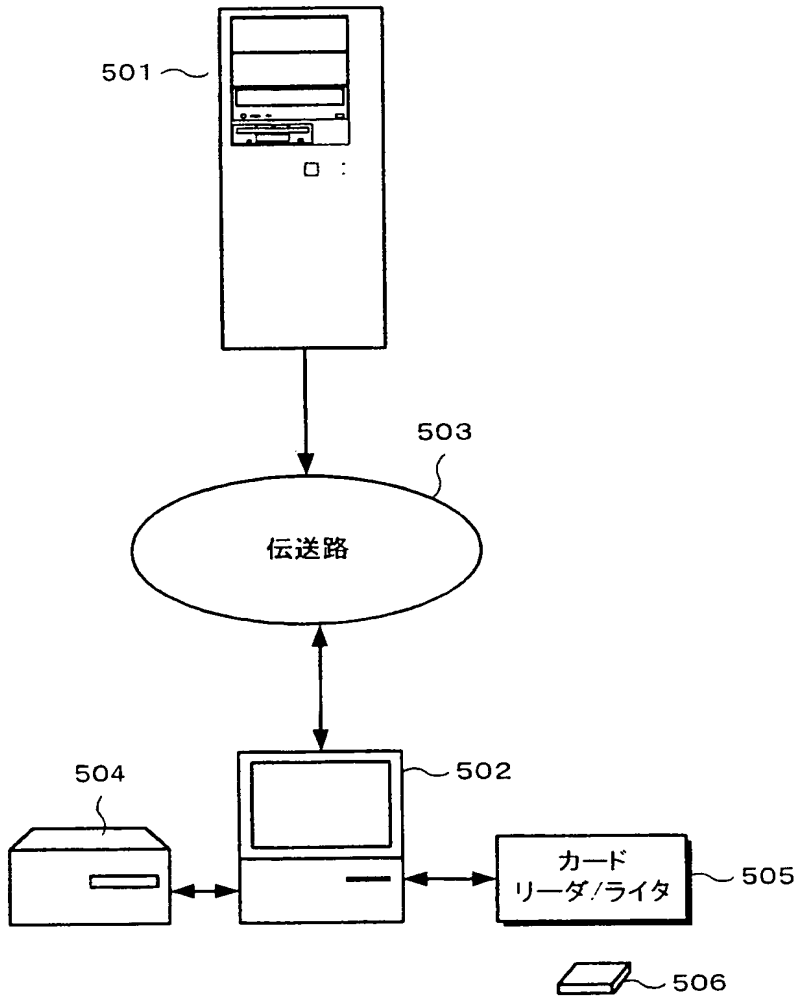
第１２図


DAコード管理
所定時間経過？
NO
S11
YES
ストレージからCキーの
DAコード呼出し
S12
DAコードは
正しい？
S13
NO
YES
S15
DAコードを更新して
ストレージに戻す
S14
コンテンツを
利用不可とする

第１３図


期限管理
所定時間経過？
S21
NO
YES
S22
ストレージからCキーのDAコード呼出し
S23
DAコードは正しい？
NO
YES
S24
DAコードを更新
S25
期限超過？
YES
NO
S26
更新されたDAコードをストレージに戻す
S27
コンテンツを利用不可とする

第１４図



１、１０１・・・コンテンツサーバ

２、１０２、２０２Ａ、２０２Ｂ、３０２・・・ユーザマシン

２０、１２０、２２０Ａ、２２０Ｂ、３２０・・・ストレージデバイス

２１、１２１、２２１Ａ、２２１Ｂ、３２１・・・暗号化／復号化処理チップ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/02404

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G06F17/60, G06F17/30, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G06F17/60, G06F17/30, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 10-13808, A (Matsushita Electric Industrial Co., Ltd.), 16 January, 1998 (16. 01. 98) (Family: none)	1-37
A	JP, 9-269916, A (Hitachi,Ltd.), 14 October, 1997 (14. 10. 97) (Family: none)	1-37
A	JP, 8-8851, A (Toshiba Corp.), 12 January, 1996 (12. 01. 96) (Family: none)	1-37

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
27 July, 1999 (27. 07. 99)

Date of mailing of the international search report
10 August, 1999 (10. 08. 99)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP99／02404

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶　G06F17／60, G06F17／30, G06F15／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁶　G06F17／60, G06F17／30, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996年
日本国公開実用新案公報	1971－1999年
日本国実用新案登録公報	1996－1999年
日本国登録実用新案公報	1994－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 10－13808, A（松下電器産業株式会社）, 16. 1月. 1998（16. 01. 98）（ファミリーなし）	1－37
A	JP, 9－269916, A（株式会社日立製作所）, 14. 10月. 1997（14. 10. 97）（ファミリーなし）	1－37
A	JP, 8－8851, A（株式会社東芝）, 12. 1月. 1996（12. 01. 96）（ファミリーなし）	1－37

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　27. 07. 99	国際調査報告の発送日　10.08.99
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5L　8724 金子　幸一　印 電話番号　03－3581－1101　内線　3560

様式PCT／ISA／210（第2ページ）（1998年7月）